White Paper

Ransomware Gangs

Who They Are And How To Defend Against Them

IRONSCALES
SAFER TOGETHER

Introduction

Ransomware is a plague on companies of all shapes and sizes around the globe, with no signs of slowing down. While progress has been made by various government agencies to identify, prosecute, and jail key members of various ransomware gangs, new gangs continue to pop up and former gangs reconstitute themselves with a new name but the same nefarious purpose.

In this guide, we will provide background details about some of the more notorious ransomware gangs and the damage they have inflicted.

Contents

Black Basta

Black Basta: Operations and Ransomware Analysis

Posts made on two underground hacking forums announced the arrival of Black Basta. These posts alluded to a fee payment in addition to a profit-sharing arrangement in return for providing corporate access credentials to a forum user by the name of Black Basta.

From an operational perspective, the tactics and techniques used in Black Basta attacks are typical of prevailing ransomware trends. The first point of note is that double extortion is a feature of attacks carried out by the gang, which reflects the now default assumption that exfiltrating sensitive data and documents before encrypting either files or devices increase the chance of receiving a ransom payment from victims.

Another notable tactic is the use of QBot malware in the attacks observed so far. Qbot is a family of backdoor trojans that also have worm features, which enable the malware to self-replicate. While Qbot's initial use was in attacks on banking systems, ransomware actors can leverage several of its features to make their work easier, including keylogging, lateral movement, and establishing persistence.

The ransomware strain eventually gets pushed out to a list of internal IP addresses on the network, most likely previously accessed using Qbot. Once the ransomware runs on a Windows endpoint system, some of the following system changes occur:

- Volume shadow copies get deleted to prevent the recovery of encrypted files.
- Windows recovery and repair features are disabled to further prevent any kind of rollback to previous uninfected system states.
- Two images get dropped into the temporary Windows folder, one of which changes the desktop background to display a message stating the computer's files have been encrypted.
- A service hijack takes over the legitimate Windows Fax service and replaces it with a malicious one that defaults to boot in safe mode. A ShellExecute API function then forces a system restart.
- The system restarts and boots in safe mode with networking, which is when the actual encryption happens.

Multithreaded encryption locks down files rapidly with the extension basta appended to them. The encryption algorithm used in these attacks is ChaCha20 with a public RSA-4096 key. This is a robust type of encryption that doesn't leave open any possibility of getting files back for free by cracking the key.

Security researchers noted a further tactical evolution in Black Basta operations when they detected variants of the ransomware strain on VMWare ESXi, which is an enterprise-class hypervisor used for running virtual machines (VMs). The variant was specifically spotted on VMs running on top of Linux servers. This targeting of infrastructure often used by enterprises demonstrates the "big game" hunting tactics of Black Basta.

Notable Black Basta Victims

By the end of June 2022, Black Basta claimed 50 victims in its list of successfully compromised companies. The typical attack profile of victims displays no common trends in terms of specific sectors or industries. Construction and manufacturing companies have been hit slightly more frequently, but nothing suggests a pattern beyond focusing on organizations located in Western nations.

The American Dental Association

The biggest name hit so far by Black Basta was the 161,000-member American Dental Association (ADA). Formed as far back as 1859, the ADA is the world's largest and oldest dental association.

In April 2022, an attack on the ADA's IT network forced a partial shutdown and signaled Black Basta's arrival on the ransomware scene. The company also had to temporarily use Gmail for email communications because internal email services were unavailable.

After the ADA initially downplayed the severity of the incident, Black Basta began leaking up to 2.8 gigabytes of ADA data on its dark web leak site. The data leak included W2 forms and accounting spreadsheets. Worryingly, some of the information was sensitive and related to ADA members who run small dental practices; businesses where cybersecurity awareness is often lacking.

Deustschen Windtechnik

Deutschen Windtechnik is a German renewable energy organization focusing mostly on wind turbines. In April 2022, Black Basta successfully infiltrated the company's IT network, which led to remote data monitoring connections to wind turbines being switched off. With increased IT/OT convergence, an additional danger posed by ransomware on industrial, energy, or manufacturing businesses is a disruption or even safety risk to key operations.

On Black Basta's leak site, a post listing Deutschen Windtechnik as a victim appeared online shortly after the attack. Each leak starts at a certain percentage, with the threat actors releasing more data as time passes and victims refuse to cave in to ransom demands. In this instance, the leak percentage for Deutschen Windtechnik reached 100%.

The Rise of Black Basta Ransomware

Claiming 36 victims within just two months of becoming operational, and at least 50 at the time of writing, it's clear the threat actors behind Black Basta know what they're doing. While nothing is definite about the identity of those behind Black Basta, there's a high likelihood this is a rebrand of one or more previously disbanded ransomware gangs, such as Conti or REvil.

There is nothing yet to indicate that Black Basta is running a ransomware-as-a-service (RaaS) operation. The underground forums that typically attract RaaS gangs recruiting new affiliates haven't yet seen any posts from Black Basta threat actors. Some potential reasons for keeping things in-house include a desire to retain all profits through highly targeted attacks on large organizations and sufficient internal technical expertise/scalability to hit targets without enlisting external affiliates. Another possibility is that Black Basta will eventually evolve into a RaaS operation.

Potential Defenses and Countermeasures

There are divisions in the security landscape on the origins of Black Basta. The professionalism and intricacy of the attacks observed so far suggest a rebranding of defunct gangs. Whatever the case, the danger is clear with Black Basta, and the victim list will only expand over the coming months. Considering the gang's operations, here are some suggested countermeasures and defenses to have in place:

- With phishing and spear-phishing emails being a common method for persuading employees to disclose passwords for business accounts/services, use dedicated anti-phishing solutions and ongoing employee cybersecurity training and awareness.
- The use of stolen dark web credentials for initial network access in these attacks once again reinforces the importance of protecting business accounts with an extra layer of authentication (two-factor or multi-factor).
- Dark web monitoring is an option that trawls the dark web for stolen employee credentials and enables you to perform hard resets on those accounts.
- Consider getting an off-site backup solution in place so that even if the ransomware strain manages to delete connected backup options, there's a way to recover files.
- Encrypt any sensitive data in your network even if encryption is not necessary for compliance with external regulations; if threat actors can't read your data, double extortion isn't effective because leaked data is encrypted.

Egregor

Egregor is a ransomware-as-a-service gang that has so far managed to claim at least 70 victims and extort tens of millions of dollars during a prolific yet short spell of operations. The Egregor ransomware strain first surfaced in September 2020, and most attacks occurred within a three-month period, ending in December 2020.

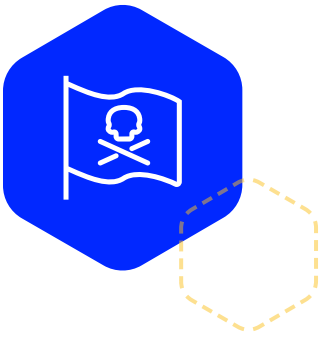
Egregor: Operations and Ransomware Analysis

As with many ransomware gangs, double extortion is a feature of Egregor's operations. Affiliates carry out attacks using Egregor's ransomware, and the leaders of the operations receive a percentage commission from any successful attack that uses their ransomware strain.

The actual ransomware strain appears to be a copy of the Sekhmet strain, which was previously used by the Maze cartel. Many industry commentators have noted that after Maze winded up its operations, several of the gang's affiliates switched to Egregor. There's a strong possibility that Egregor is a rebranding of Maze by some of the operation's former leaders.

Initial access stems from a variety of methods, including using stolen credentials, hacking remote access technology, and conducting spear-phishing campaigns with malicious attachments targeted at specific employees. Threat actors use the threat emulation toolkit Cobalt Strike to covertly discover information about their victim's network and move laterally.

The code itself uses obfuscation techniques to evade analysis and detection by security solutions. PowerShell scripts attempt to uninstall or disable popular endpoint security solutions. After exfiltrating data, the payload executes, and victims receive a ransom note demanding payment within a three-day window to avoid having their data leaked online.



High-Profile Egregor Attacks

Barnes and Noble, October 2020

Bookstore giant Barnes and Noble became one of Egregor's most high-profile early victims in October 2020. A public statement by Barnes and Noble disclosed the fact that a cyber attack resulted in unauthorized and unlawful access to certain Barnes & Noble corporate systems.

Acting from a position of caution, Barnes and Noble advised that some customers may have had their data compromised. The compromised data potentially included email addresses, shipping addresses, and telephone numbers. A post appeared on Egregor's dark web leak site shortly after with apparent proof of stolen data.

Crytek and Ubisoft, October 2020

In somewhat of a double-whammy attack, video game developers Crytek and Ubisoft were two unfortunate organizations counted among Egregor's earliest victims. Two posts appeared on Egregor's dark web leak site simultaneously with purported files and data exfiltrated from both companies' IT systems.

The Ubisoft leak contained source code from one of the company's video games while the Crytek leak featured developmental resources for upcoming games. After being contacted by ZDNet, Egregor confirmed that they had only stolen data from Ubisoft; systems were left untouched and unencrypted by ransomware. Several of Crytek's systems, however, were encrypted fully by Egregor threat actors.

Kmart, December 2020

Kmart is an American department store chain that has experienced troubling times in recent years. Despite respectable annual revenues of almost $10 billion in 2020, Kmart continues to feel the impact of customers favoring online shopping. In early December 2020, a ransomware attack impacted back-end IT services at the company. A human resources website owned by parent company Transformco went offline following the attack.

The Holiday season is a particularly important time of the year for retailers. Threat actors know that successful attacks on retailers' IT systems conducted during the busiest time of the year have a higher likelihood of leading to payouts. Security researchers who saw the ransom note from this incident confirmed that the Egregor operation was behind the attack. Kmart never publicly commented on the ransomware incident, and it appears the damage was limited to encrypted back-end servers and workstations.

Egregor has used phishing emails to gain initial access to networks

Translink, December 2020

Translink operates the regional transportation network of Metro Vancouver. With over 6,900 employees, the statutory authority manages a range of critical modes of transit, including buses, SkyTrain, and commuter railway services. In another early December 2020 attack, the Translink incident affected phone services, online services, and payment systems. Customers temporarily couldn't pay for transport services with credit or debits cards.

The ransom note requested payment within three days if Translink wanted to avoid its data being published online. Egregor opted for an interesting method to deliver the ransom note to Translink; hijacking printers and repeatedly printing out the note. This tactic echoed an attack carried out by Egregor two months previously on Chilean retail giant Cencosud.

Future of Egregor

In what's been a busy year busting ransomware gangs for Ukrainian law enforcement, a joint operation with French authorities resulted in the arrest of several individuals associated with the Egregor operation. The February 2021 swoop caught suspects who were Egregor affiliates carrying out hacks using the gang's ransomware strain.

At the time of the arrests, the dark web leak site operated by Egregor went offline. Whether this sudden departure represents the operation's leaders becoming spooked or the Ukrainian law enforcement sting was more far-reaching than reported remains unknown. CSO reported that the leader of Egregor may have been arrested when the authorities closed in.

There's a chance that Egregor will re-emerge under a new name, and that this absence represents a hiatus. The other possibility is that Egregor has been shut down permanently. Only time will tell whether Egregor has any future or it's been consigned to history. Organizations still need to remain cautious in preventing ransomware attacks because there are always new threat actors looking to get a slice of what is a very large pie.

Blocking Spear Phishing

Like many ransomware gangs, Egregor has used phishing emails to gain initial access to networks. These emails have been highly targeted spear-phishing emails sent to specific individuals about whom the threat actors gleaned information on social media, company web pages, and other sources. Typically, these emails come with attachments containing malicious payloads that enable hackers to infiltrate a network.

Successfully blocking phishing emails provides robust defense against today's ransomware attacks. A dedicated email security platform with anti-phishing capabilities can prove a game-changer in becoming the next ransomware victim or keeping hackers at bay.

DoppelPaymer

DoppelPaymer is a ransomware gang that extracts data from victims' systems and then encrypts those same systems. Named after the strain of ransomware that the gang deploys, DoppelPaymer has demonstrated ruthlessness in its choice of victims with no industry safe from its targeting. This article analyzes DoppelPaymer's operations, ransomware strain, and some of its high-profile attacks.

DoppelPaymer: Operations and Ransomware Analysis

DoppelPaymer first emerged in 2019, and security researchers immediately noted that the ransomware strain appeared to build on BitPaymer, which began targeting healthcare organizations in 2017. Some security analysts link DoppelPaymer back to the Russian threat-actor TA505.

In terms of how the gang operates, threat actors favor malicious email attachments as the initial vector for infiltrating a victim's network. Typically, these are highly targeted spear-phishing emails that make victims more likely to open attachments under the guise that the emails come from a trusted source.

When someone at a target organization opens the malicious email attachment, the Dridex trojan downloads onto their system. Leveraging Dridex and opening affected systems to incoming connections, the threat actors then download other tools, including a PowerShell exploitation agent, a credential dumping tool, and threat emulation software.

Leveraging stolen credentials, lateral movement, and evasive detection techniques, the DoppelPaymer ransomware eventually executes on systems. The gang uses a tool known as ProcessHacker to terminate different services on endpoint devices. Multiple systems are locked simultaneously, and victims receive a ransom note with payment instructions linking to a dark web payment portal.

High-Profile DoppelPaymer Attacks

Kia Motors America: February 2021

The United States division of South Korean multinational automobile manufacturer Kia became a high-profile DoppelPaymer victim in February 2021. This ransomware attack impacted payment services, internal dealership systems, and a mobile app used by the company.

As is par for the course in DoppelPaymer attacks, this was a double extortion incident. The threat actors demanded $20 million in Bitcoin if Kia Motors America wanted to avoid having stolen data leaked online. Despite BleepingComputer getting access to the ransom note used in the attack, Kia denied that it had suffered from any ransomware incident. A statement made to BleepingComputer referenced an extended systems outage.

Foxconn: December 2020

Foxconn is one of the world's largest providers of electronics manufacturing services. The Taiwanese multinational company has over 1.2 million employees globally. A December 2020 attack on Foxconn again highlighted the scope of DoppelPaymer's ambitions in targeting some of the world's major companies.

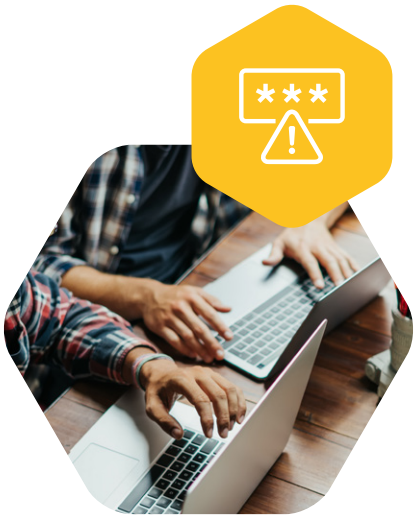
The successful ransomware attack encrypted over a thousand of Foxconn's servers and exfiltrated over 100 gigabytes of data. The attack targeted a location in Mexico housing a facility for the company's North and South American operations. An interesting aspect of this attack was how the DoppelPaymer threat actors went out of their way to destroy 20-30 gigabytes of data backups presumably to further increase the probability of getting paid.

Considering the size of Foxconn, the ransom note left by DoppelPaymer demanded $34 million in Bitcoin. Only servers rather than employee workstations were encrypted. DoppelPaymer published files claimed to belong to Foxconn shortly after the attack, but Foxconn couldn't confirm the authenticity or ownership of those files.

Boyce Technologies: August 2020

In a disturbing example of DoppelPaymer's merciless approach to cyber attacks, ventilator manufacturer Boyce Technologies suffered a ransomware attack in August 2020. This month marked a tumultuous period worldwide with the Covid-19 pandemic wreaking havoc on countries like the United States.

Boyce Technologies supplied vital ventilators to hospitals and healthcare facilities in New York that helped to deal with the worst cases of the virus. This incident became public knowledge when DoppelPaymer released a post with samples of files it had stolen from Boyce Technologies on its dark web leak site. A threat to release a lot more data accompanied the post.



Newcastle University: August 2020

Newcastle University is a public research university in the northeast part of England. Notable alumni include actor Rowan Atkinson and UK Royal Family member Princess Eugenie. In August 2020, Newcastle University's IT systems were heavily disrupted by what turned out to be a DoppelPaymer attack.

The incident caused severe operational disruption across networks and IT systems used by the university. A public update released one week after the attack indicated the damage would take several weeks to address. Students could only access a limited number of IT services, which negatively impacted their ability to study course materials. Following the attack, the threat actors began leaking sensitive information online, including Newcastle University students' home addresses, phone numbers, and personal email addresses.

DoppelPaymer: FBI Alert, Rebranding and Future

The extent of DoppelPaymer's operations and victim profiles prompted the FBI to release a warning in December 2020 that the gang was targeting critical infrastructure. The alert advised victims not to pay a ransom to criminal actors.

An interesting part of the alert was the FBI's observation that DoppelPaymer was one of the first gangs where threat actors have called the victims to entice payments. This harassment aligns with the generally brutal nature of DoppelPaymer's operations. Among the FBI's recommended mitigations were having secure backups disconnected from the network and setting alerts for data exfiltration.

Perhaps in part due to the FBI setting its sights on DoppelPaymer, a lull in the gang's operations started midway through 2021. No new leaks were posted on the dark web leak site for over a month.

Security researchers found that the group rebranded in May 2021 under the new name Grief. An early sample of the Grief ransomware strain linked to DoppelPaymer's portal. Updated versions now link to a new portal that has extremely close similarities in layout to the DoppelPaymer portal.

There is no doubt that this is a rebranding of DoppelPaymer. And given the nature of the gang's operations, this is a worrying development that shows they are not going away.

Preventing Successful Spear Phishing Attacks

Given the information known about how the DoppelPaymer threat actors operate, it was interesting to note that the FBI's alert didn't contain any reference to spear-phishing when discussing mitigation strategies. In fact, the word phishing didn't appear at all in the document.

Given the widespread use of malicious Office documents as email attachments in instigating DoppelPaymer attacks, it's worth addressing spear-phishing as a mitigation strategy. If you can prevent people from opening malicious attachments, you can stop adversaries in their tracks before they infiltrate your network.

Traditional security solutions struggle to detect spear-phishing emails. Furthermore, because of their highly targeted nature, these emails are very convincing. Threat actors can leverage company profiles and social networking platforms to obtain information about specific employees, such as executives.

Dealing with the threat of spear phishing requires a multi-pronged approach, but such an approach can make the difference in avoiding the devastating effects of ransomware attacks. Phishing simulation and training can help employees at all levels of seniority to better recognize phishing emails. While training and simulation aren't guaranteed to stop people from being duped, they are effective methods to reduce that risk.

Another crucial tenet of dealing with spear phishing is having a dedicated email security platform that automatically detects, investigates, orchestrates, and responds to suspicious emails. Ideally, your email security solution would have sandbox engines to identify and isolate emails that contain malicious links and attachments.

Netwalker

Netwalker is a notorious name on the ransomware scene with a prolific record of successful attacks. An estimated $25 million in ransom extortions between March and September 2020 established the gang as a force to be reckoned with. This article looks at Netwalker's operations, the specifics of the ransomware variant, and some high-profile attacks carried out using Netwalker ransomware.

Netwalker: Operations and Ransomware Analysis

Like many modern money-motivated ransomware gangs, Netwalker extended its reach (and profits) by running a ransomware-as-a-service operation. Advertisements for criminal affiliates to use Netwalker's ransomware emphasized the importance of experience with infiltrating complex IT networks. The ability to speak Russian is another notable requirement to become a Netwalker affiliate.

Netwalker's members use double extortion tactics to increase pressure on victims by threatening to publish their data online if they don't meet ransom demands. When recruiting new affiliates, dark web advertisements have indicated a preference for threat actors who already have a foothold inside corporate networks. This foothold makes data exfiltration (and by extension double extortion) more likely.

Netwalker threat actors typically establish initial network access by running phishing and spear-phishing campaigns. A VBS script attached to these emails establishes an initial foothold into the infected machine. Then, the ransomware replaces legitimate processes with the malicious payload, which enables it to lurk inside systems and networks and easily evade detection by both users and anti-virus tools.

Like several other ransomware variants, Netwalker deletes Volume Shadow copies of files so that victims can't restore encrypted files from those copies. Interestingly, a batch script created after encryption attempts to delete samples of the ransomware from local machines in a definite effort to evade analysis by security researchers.

Ransom notes left on victim computers instruct them to contact the gang via the Tor web browser using a victim-specific code. After paying the proposed ransom by Bitcoin, victims are able to download a decryption tool that removes the Salsa20 encryption cipher used by Netwalker.

Netwalker Attacks

University of California – San Francisco

In June 2020, Netwalker successfully attacked the University of California San Francisco (UCSF). The university is a global leader in biological and medical research with both a medical school and a medical center. The June 2020 attack encrypted several UCSF servers, which contained important data related to academic research.

This was a particularly high-profile incident not just due to the victim in question but also because the UK's BBC News managed to follow the ransom negotiations live on the dark web. The university countered an initial demand for $3 million with an offer of $780,000, which Netwalker threat actors denigrated as "a very small amount for us." Eventually, UCSF negotiators transferred $1.14 million in Bitcoin to Netwalker in return for a decryption tool.

Toll Group

Toll Group is an Australian transportation and logistics company with reported revenue totaling $7.8 billion dollars in 2020. In February of the same year, Toll Group became one of the earliest known victims of Netwalker ransomware. The incident caused delays and disruptions to the organization's operations.

This attack occurred just before Netwalker switched to a RaaS operation from its previous, smaller-scale model. Luckily for Toll Group, data exfiltration wasn't prioritized by Netwalker members at the time, so no sensitive data was lost or stolen.

Reports suggested the Netwalker ransomware variant spread to over 1,000 Toll Group servers. In another blow to the company, Nefilim ransomware infiltrated its network just a few months later. Two network compromises in such a short space of time point to ineffective cybersecurity practices and solutions. Nine months after the initial Netwalker attack, a company spokesperson indicated Toll Group was still dealing with the fallout from both ransomware incidents.

K-Electric

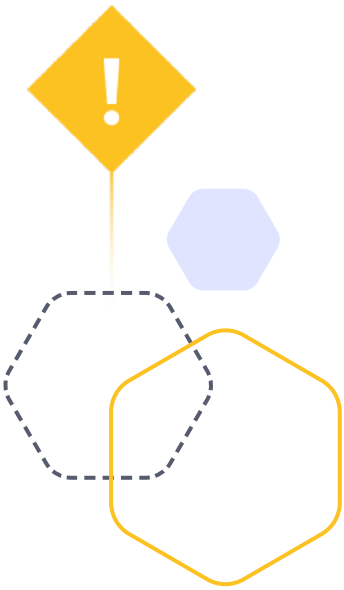
K-Electric is an electric supply company in Pakistan with over 10,000 employees. Established in 1913, K-Electric is Pakistan's largest private sector power supply company. In September 2020, Netwalker threat actors executed the gang's variant on K-Electric's IT network, which disrupted billing services for customers. The ransom message demanded $3.8 million in Bitcoin with a threat to increase to $7.7 million if K-Electric executives didn't pay up.

A statement given by K-Electric to BleepingComputer following the incident outlined that customer data remained intact and secure. This seemed to conflict with a message on Netwalker's dark web leak site that alluded to stolen unencrypted files from K-Electric's network. Sure enough, after K-Electric refused to pay up, Netwalker released 8.5 gigabytes of stolen data financial data, customer information, and engineering reports.

This attack served as a stark reminder that ransomware gangs aren't bluffing when they threaten to publish stolen sensitive data online. The lack of transparency from K-Electric about exfiltrated data was also concerning. There is a chance that the company didn't know copies of sensitive files were taken from the network, but the message communicated seemed definitive in concluding that customer data remained secure.

Weiz, Austria

A May 2020 attack on the municipality of Weiz in Austria exemplified the diverse set of targets within the sights of Netwalker threat actors. The incident saw Netwalker ransomware installed on computer systems that were part of the area's public network. As an important economic hub with several large companies housing production plants there, the attack perhaps had a more ambitious motive, such as stealing sensitive information belonging to those companies.



Arrest and Dark Web Site Seizure

In January 2021, Canadian police arrested a Netwalker affiliate named Sebastien Vachon-Desjardins and seized almost $500,000 in cryptocurrency payments made to him. In what was a collaborative effort from international law enforcement involving the FBI and Bulgarian authorities, Netwalker's Tor website was also seized.

A U.S. Department of Justice statement highlighted how law enforcement is, "striking back against the growing threat of ransomware by not only bringing criminal charges against the responsible actors, but also disrupting criminal online infrastructure and, wherever possible, recovering ransom payments extorted from victims."

It's unclear whether Netwalker will return under another moniker, but there has been no evidence of the gang's operations resuming yet. The law enforcement effort only managed to arrest an affiliate of the gang, which suggests the remaining members are still out there. Perhaps they're content with the money they managed to make from previous incidents.

Covid-Related Phishing Threats

Netwalker operators adjusted their phishing campaigns to account for the Covid pandemic. The gang members clearly believed that exploiting the uncertainty created by Covid would increase the chances of luring victims into opening malicious email attachments.

These attachments appeared to contain information about the latest Covid updates coming from legitimate sources. The reality was that they contained malicious attachments that initiated the spread of ransomware attacks by executing malicious payloads and scripts. The estimated $25 million in ransom payments collected at the height of the pandemic by Netwalker backs up the effectiveness of this tactic.

These Covid-related phishing threats demonstrate the extent to which ransomware gangs will adjust their tactics for maximum devastation. Even as the crisis winds down, it's always worth remembering that threat actors constantly lurk and seek to exploit moments of crisis and uncertainty. As many companies shift to a full-time hybrid work model, phishing emails exploiting work-from-home setups will undoubtedly remain a constant threat.

Businesses need an advanced email security solution if they are to stand a chance of mitigating phishing threats. While it's possible to train employees to recognize phishing emails, it's only human that people get conned when they are living through unprecedented times. An advanced email security solution fights phishing from the frontline using self-learning, AI-driven technology.

Clop

Clop is a ransomware gang that first appeared in February 2019 when security researchers found new ransomware strains with the .Cl0p extension. A spate of prolific and high-profile attacks within a short period of time ensured the gang quickly made a name for itself. This article analyzes Clop's operations and highlights some high-profile attacks carried out by the gang.

Clop: Operations and Ransomware Analysis

The gang's members are Ukrainian, and they previously used a ransomware strain known as CryptoMix. The initial attack vector that provides access to a victim's network is often a spam email, notification about fake software updates, or a more targeted spear-phishing campaign. After a victim downloads a malicious file, such as a macro-enabled email attachment, the group then deploys reconnaissance, lateral movement, and data exfiltration techniques before finally delivering a ransomware payload that encrypts affected systems.

Despite security researchers detecting Clop ransomware in February 2019, the group's dark web leak site didn't appear online until over one year later in March 2020. This leak site creates extra pressure on victims to pay up by publicly disclosing small samples of stolen data.

This ransomware strain tries to evade detection on endpoint systems by attempting to disable Windows Defender and remove other Microsoft security tools found on devices running older operating systems. The point at which ransomware is about to be installed is often too late in the game, however, organizations with Windows 10 can defend against attempts to disable Windows Defender by ensuring Tamper Protection is switched on for all endpoint devices connected to the network.

Unlike several of today's other well-known ransomware gangs, Clop doesn't operate a ransomware-as-a-service model. The group carved its own path and decided to keep all profits for its members, which indicates a relatively large operation.

High-Profile Clop Attacks

Utility Trailer Manufacturing, May 2021

Utility Trailer Manufacturing designs and manufactures refrigerated freight vans, flatbed trailers, and other semi-trailers. In business since 1914, the company is the leading refrigerated trailer manufacturer in the United States.

In May 2021, the company suffered a cyber attack that temporarily disrupted systems and resulted in sensitive data exfiltration. A post on Clop's dark web leak site disclosed up to five gigabytes worth of personal information about Utility Trailer's employees. The leaked data included compensation claims, termination records, and even tax forms. Often, these initial leaks represent a small snippet of the exfiltrated data; threat actors hope to scare victims into paying up so that more of their data doesn't make it to the public domain.

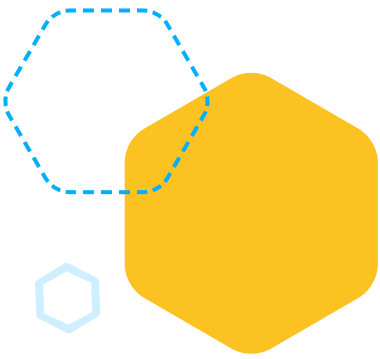
Shell, March 2021

Oil giant Shell became arguably Clop's most high-profile victim as part of a supply chain attack that impacted multiple organizations around the world. The incident occurred when Clop managed to compromise the Accellion file-sharing service with the aid of another threat group known as Fin 11.

The Shell incident didn't result in any IT disruptions for the oil and gas producer because Clop opted not to install its ransomware strain on any systems. This was an attack that solely focused on exfiltrating sensitive data and demanding a ransom for it. Shell disclosed the attack in March 2021, but the data exfiltration probably happened a few months prior. Posts on Clop's dark web leak site showed passport scans belonging to Shell employees among the stolen data.

University of Colorado, March 2021

The University of Colorado also impacted by the same supply chain cyber attack as Shell. Details of students' grades and social security numbers from the school began appearing online in March 2021, which aligned with the university's public disclosure a month previously that it was impacted by the Accellion file transfer service breach. Reports suggest that the Clop gang demanded a $10 million ransom payment to prevent further data leaks.



Symrise, December 2020

In an incident bearing the hallmarks of a more traditional double extortion attack, German flavor and fragrance developer Symrise AG became the latest Clop victim in an attack that took place in December 2020. After almost 1,000 devices became unusable due to encryption, Symrise had to halt production and shut down IT systems to contain the spread of ransomware.

Before spreading its ransomware strain in Symrise's network, the Clop gang managed to exfiltrate 500 gigabytes of unencrypted files from Clop's IT systems. Once again, Clop used its dark web leak site to post details of stolen files to entice Symrise to pay up.

E-Land Retail, November/December 2020

E-Land Retail is part of a South Korean conglomerate that produces and distributes consumer goods, including apparel and housewares. In November 2020, a company statement revealed that E-Land Retail was the latest victim of Clop's targeted ransomware attacks. According to the statement, a compromised server had to be shut down.

Just one month later, further details emerged stating Clop gang members managed to infiltrate E-Land Retail's network up to one year before the ransomware incident. During this initial infiltration, threat actors managed to install malware on Point of Sale (POS) systems. This malware enabled the gang to steal credit card details belonging to up to two million E-Land retail customers.

This attack demonstrates how evasive threat actors can lurk for lengthy periods in your network before eventually striking servers and other critical systems with their ransomware payloads.

Software AG, October 2020

In another Clop attack hitting a German company, prolific software development company Software AG fell victim to the gang's operations. A press release mentioned that internal Software AG systems were impacted by the attack but that customer-facing services were unaffected.

The hackers also managed to get their hands on company data in the attack on Software AG, which led to a substantial ransom demand of approximately $23 million. Mirroring previous double extortion incidents in which victims refused to pay up, Clop's members soon began releasing data on the dark web. The leaked data included details about some of Software AG's near 5,000 employees.

The Demise of Clop

In June 2021, it appeared that Clop became a victim of its own success in targeting large organizations. Authorities in Ukraine closed in and apparently arrested six of the gang's members as part of a collaborative effort involving international law enforcement and the Binance cryptocurrency exchange. South Korean and US authorities were also involved, which perhaps reflects the fact that major organizations in these countries were victims of Clop's operations.

The role of Binance appears particularly significant in that its behavioral analysis on crypto transactions uncovered details of over $500 million in laundered ransom payments, which helped with tracking down the perpetrators.

A press release published by Ukrainian authorities indicated a degree of closure to Clop's operations in that they alluded to shutting down the gang's infrastructure. However, six days after the arrests, one prominent cybersecurity reporter Tweeted that a new victim appeared on Clop's ransomware leak site. The operation to take down Clop appears to have been unsuccessful. It's likely that the people arrested did not include all core members of the gang.

Babuk

Babuk is a new ransomware gang that emerged in early 2021. The gang's initial mission statement referenced a non-malicious intent to conduct ransomware attacks as an apparent audit of the security of corporate networks. The reality of Babuk's operations, however, does not align with this non-malicious intent, as the gang has exfiltrated sensitive data from organizations in law enforcement and others. This article analyzes Babuk's operations, ransomware strain, and victims.

Babuk: Operations and Ransomware Analysis

Babuk began operating a ransomware-as-a-service gang like higher-profile gangs such as DarkSide. Dark web forum posts written in both Russian and English indicate a Russian origin for Babuk. Advertisements posted on the dark web attempt to recruit affiliates with penetration testing skills who can use the Babuk ransomware strain to hack corporate networks and share a proportion of any ransom payment with Babuk's leaders.

Further delving into the apparent benevolent nature of their intentions to "audit the security of large corporate networks", the gang specified an unwillingness to attack hospitals, non-profits, and companies earning less than $4 million in annual revenue. This victim selectiveness demonstrates an attempt to make out that Babuk are the good guys, but the gang didn't fool anybody in the security world, particularly when racist sentiments appeared on some forum posts made by the gang's members.

The first point of note about Babuk's ransomware is the relatively primitive, unsophisticated nature of its code. Security researchers who first spotted Babuk noted some technical errors in the binaries of the code, and they speculated these errors stemmed from attempting to create a cross-platform strain that infected Linux, Unix, and vmware systems. Encryption tends to perform slowly due to poor coding in Babuk ransomware. The decryption tool used by Babuk was so riddled with errors that encrypted files couldn't be retrieved even if victims paid the ransom.

Typical Babuk ransomware attacks include tactics such as checking currently running processes on systems and killing those processes that can detect it. Babuk ransomware also destroys shadow volume copies of machine storage volumes. Encryption runs using the ChaCha algorithm, and victims can only get their files back if Babuk supplies a private key for decryption.

Large similarities exist between Babuk's ransomware and that of another operation named Vasa Locker. These similarities stretch as far as almost identical ransom notes, the same file extension added to encrypted files, and the same encryption method.

Babuk's Victims

Security researchers believe Babuk managed to successfully attack up to five large corporate networks so far. From these successful attacks, three victims are publicly known.

Washington DC Metropolitan Police Department

Any cyber attack managing to infiltrate the network of a police department rightly warrants attention. Babuk operators received global media attention in April and May 2021 when details emerged of a ransomware attack on the Washington, D.C. Metropolitan Police Department.

A dark web post on Babuk's leak site claimed the gang managed to breach the police department's IT network and exfiltrate 250 gigabytes of data. Babuk demanded a ransom payment of $4 million. After the police department refused to cough up the full amount, Babuk published the full trove of data on its leak website.

Published data included social security numbers belonging to members of the police department and lists of persons of interest kept on file by Washington D.C. Metro Police. Babuk referred to an offer of $100,000 made to the gang to avoid the publishing of stolen data, but this amount was too low. It's unknown whether the incident resulted in locking down computer systems using Babuk's ransomware strain or whether this was solely a data exfiltration attack.

Houston Rockets

The Houston Rockets are a team in the NBA (National Basketball Association). Babuk targeted this professional basketball team with its ransomware strain in April 2021. Statements made to the media at the time reported that "internal tools prevented ransomware from being installed except for a few systems that have not impacted our operations."

The relatively limited impact of the ransomware strain on Houston Rockets' internal IT operations didn't prevent this from being a severe attack, though. Following the news of the incident, Babuk claimed to have stolen 500 gigabytes of data belonging to the Houston Rockets. This data included highly sensitive documents, such as contracts and non-disclosure agreements. Modern ransomware gangs favor these double extortion attacks because they put added pressure on victims to pay up and ensure their sensitive information remains private.

Serco

Serco is a contractor used by the British government to deliver important services to citizens, such as management services at NHS hospitals, test and trace for Covid-19, and border security services. In January 2021, Serco confirmed it was hit by a double extortion ransomware attack orchestrated by the Babuk gang. This confirmation of the attack followed Babuk's publicly claiming Serco as a victim three months previous.

The incident targeted Serco's IT infrastructure in mainland Europe. The company entered negotiations with Babuk hackers, although it remains unclear whether any ransom payment exchanged hands. Organizations such as NATO and the Belgian military, with whom Serco was a contractor, sought assurances that their data remained secure and private. The ransom note indicated threat actors lurked inside Serco's network for three weeks and exfiltrated up to one terabyte of data.

Babuk's Future: Exit, Conflict, and Realignment of Operations

After a brief but damaging spell of operations, Babuk's leaders signaled an intention to retire via a dark web post. This message spelled out that the Babuk project would be closed, and the ransomware's source code made publicly available. Interestingly, the intention to cease operations came in the wake of media headlines about Babuk hacking the Washington D.C. Police Department. Perhaps the heat from law enforcement prompted a shutdown like how REvil vanished when the FBI closed in.

Following the shutdown, the media reported that one Babuk member said the gang split up after internal conflict emerged in the aftermath of the Washington Police incident. One member wanted to publish all the stolen data while others were reluctant due to the attention this would likely attract from more cyber-aware organizations like the FBI.

One month after the internal conflict began, several current Babuk members reestablished Babuk version 2. A dark web message posted in May 2021 clarified a realignment of operations away from classic ransomware attacks involving encryption to solely focus on data exfiltration.

In another interesting development, a member of the Babuk group eventually released the full source code for the ransomware strain on a Russian hacking forum in September 2021. Security researchers used this information to create a decryption tool for any Babuk victim to decrypt infected systems.

Defending Against Initial Babuk Attack Vectors

Babuk uses similar attack vectors as many other ransomware gangs to gain initial access to corporate IT networks. Email phishing campaigns containing malicious attachments, exploiting software vulnerabilities, and hacking remote desktop protocol (RDP) appear to be the three main initial modes of access. Preventing this initial access is critical in stopping ransomware attacks in their tracks before they lock down systems or manage to extort your sensitive data.

Here are some tips for defending against these 3 attack vectors:

Phishing

Get a dedicated anti-phishing email security solution in place and train employees on how to better spot phishing emails.

Common Software Vulnerabilities

Establish a dedicated patch management strategy that ensures all applications and services used in your IT network are regularly updated.

RDP

Require multi-factor authentication for logins so that remote users need to provide an additional category of evidence to verify who they are before logging in.

FIN7

FIN7 is a unique group in the shady world of cybercrime. Infamous for sophisticated stolen credit and debit card hacks involving phishing emails and other social engineering methods, the gang's threat actors deploy a range of constantly evolving tactics to steal money; the latest of those tactics is ransomware. This article overviews FIN7's operations.

FIN7: Operational Analysis

FIN7 is a large-scale cyber gang with more than 70 employees organized into different business units. Some units develop malware to infect point-of-sale (POS) systems and help steal payment card information. Other units focus solely on the task of crafting convincing phishing emails that entice unsuspecting people into opening malicious attachments.

FIN7 gained infamy for a series of attacks on banks and financial institutions starting in 2013. While no official figures are available, some sources claim the gang managed to steal $900 million using hacking methods that targeted ATM networks. After establishing command and control, the threat actors instructed ATMs to dispense cash, which money mules collected and transferred to FIN7's members' bank accounts. Some security researchers aren't quite certain that FIN7 was behind this set of attacks on banks, and there may have been another entity involved.

The gang gained further notoriety during 2015 for multiple attacks on retail outlets, hotels, casinos, fast-food restaurants, and other businesses with high volumes of POS transactions. After establishing a foothold into a network using a malicious email attachment, FIN7 threat actors installed Carbanak malware, which helped harvest card details from well over 6,500 POS systems.

FIN7's initial operations were so prolific that businesses in all 50 US states became victims of these attacks. Estimates put the total number of stolen payment cards at 16 million. Typically, threat actors listed these stolen card details for sale on dark web marketplaces. People who bought the stolen cards used them to make standard online retail purchases or to purchase gift cards.

FIN7 On the Ransomware Bandwagon

FIN7 is a prime example of the opportunism at play in the world of cybercrime. Threat actors alter and evolve their attack methods in line with what works and what's most profitable. FIN7 appears to have jumped on the ransomware bandwagon within the last couple of years. Given FIN7's propensity for financially motivated attacks, it's not a big surprise to see the gang shift to ransomware to further increase profits.

An investigation by Truesec in December 2020 detailed a cyber-attack in which typical FIN7 tools, including the Cabarnar remote access trojan, were used to establish a foothold in a victim's network. In the same attack, threat actors installed Ryuk ransomware on the victim's computers. Ryuk runs a prolific ransomware-as-a-service operation, and FIN7 threat actors may well have signed up as affiliates in what looks like a particularly dangerous partnership.

In a bizarre attempt to recruit security professionals to carry out parts of their ransomware operations, FIN7 leaders created a fake penetration testing company named Bastion Secure. The recruitment phase for job advertisements at the phony company involved applicants conducting a real penetration test on one of Bastion Secure's "customers". Instructions to applicants told them to specifically use tools that couldn't be detected by security software and to check for file backups once inside the network.

A more recent update about FIN7's ransomware operations came in January 2022. The FBI warned that FIN7 threat actors began sending malicious USB drives to a range of businesses in August 2021. These drives were packaged to look like they came from legitimate sources, such as Amazon, and they included a thank you letter. Other drives were packaged to look like they contained Covid-19 related information shipped by the US HHS.

When an unsuspecting employee inserts the drive into their computer, the malicious USB loads itself on the computer as a keyboard. Preconfigured keystrokes execute PowerShell scripts that install backdoors into the network. Eventually, threat actors deploy ransomware strains including REvil and BlackMatter.

An advanced email security solution provides the defense needed to accurately detect and mitigate phishing threats

FIN 7 Arrests

In February 2021, Fedir Hladyr, a Ukrainian national, received a ten-year prison sentence for his role as the systems administrator for FIN7. German police arrested Hladyr three years previously in Dresden and they extradited him to the United States. The Ukrainian played a key role in FIN7's operations, but such is the large-scale nature of the gang's operations that losing a key member didn't stop the threat actors in their tracks. Two other Ukrainian members of FIN7 were also arrested around the time of Hladyr.

Elaborate Phishing Schemes

Phishing emails underpinned the success of FIN7's cyber-attacks. With an entire unit of the gang dedicated to crafting phishing schemes, it's easy to see how they managed to lure some victims into opening their malicious email attachments. Without this social engineering ability to gain an initial entry point into victims' networks, none of the more sophisticated tactics used by the gang would have succeeded.

A US government document features two examples of FIN7 phishing emails. In one case, a restaurant worker opened a malicious attachment from an email claiming to be a customer order. The email body states that "the enclosed document contains the order and my personal info". While a seasoned security professional wouldn't have opened this attachment, restaurant workers are not typically security aware. Choosing the right targets is as much a factor in FIN7's phishing success as choosing the right message.

Regardless of the target or the message, stopping elaborate phishing schemes in their tracks calls for advanced email security solutions. Educating employees in recognizing the signs of phishing is useful, but an advanced email security solution provides the defense needed to accurately detect and mitigate phishing threats.

Blackcat

International law enforcement collaboration led to the disbandment of several high-profile ransomware gangs in the last 12 months. As ransomware attacks gained more media coverage and wreaked more havoc on critical industries, these threat actors became much-sought targets for authorities. The biggest story came in January 2022 when Russian authorities closed in on REvil and claimed that the gang has "ceased to exist".

The story of a ransomware gang regularly seems to end with its arrest or sudden disappearance from the web in recent times. However, warnings in previous posts highlighted that the tale of many disbanded gangs probably wasn't over. It appears this warning has come to fruition with the emergence of a new group named BlackCat (also known as ALPHV). This article rounds up the series on ransomware groups by analyzing the new BlackCat operation.

BlackCat: Operations and Ransomware Analysis

Even when authorities close in on a group of threat actors, they don't necessarily arrest all of them. Furthermore, the predominance of the ransomware-as-a-service model means that there are often many affiliates associated with these gangs. Affiliates may join and start their own group or join a new group.

Security researchers first observed BlackCat activity in November 2021. An immediate point of note about their operations is the use of triple extortion in some attacks. This evolution on double extortion adds the threat of a DDoS attack on a victim's network if the victim refuses to pay the ransom. On top of the standard data exfiltration and ransomware files locking key systems, triple extortion adds another layer of pressure to pay up.

Lucrative affiliate offers are another distinct feature of BlackCat's model. Recruitment posts on Russian language forums offered affiliates up to a 90% share of any ransoms collected. The ransomware strain itself is written in Russian.

Threat actors signing up as affiliates get access to the ransomware strain. Typically, affiliates use common tactics and procedures to gain initial network access and move laterally. Privilege escalation features are embedded in the ransomware. After executing the payload, the encryption uses AES128-CTR and RSA-2048 algorithms.

BlackCat developers coded their ransomware using the Rust programming language. Rust has good cross-platform functionality, which makes it trivial to create variants that work on both Windows and Linux operating systems. Furthermore, the customizability of the language means threat actors can tailor attacks to specific victims' networks.

The common trend running through BlackCat's operations and ransomware strain is its innovation. This is evidently an experienced group of threat actors with sophisticated cybersecurity knowledge.

BlackCat's victims

An aggressive set of attacks conducted in a short timespan meant BlackCat gained rapid notoriety in the cybersecurity community. In a timespan stretching just over one month, more than 12 victim names appeared on the gang's dark web leak site. This prolific start to operations catapulted BlackCat straight into the top ransomware threats.

Moncler, December 2021

Italian luxury fashion giant Moncler became a high-profile BlackCat victim in December 2021. Formed in 1952, the company has over 1,400 employees and earns annual revenue of €1.4 billion.

The attack on Moncler unfolded when the company announced a disruption to IT operations on December 23. News filtered through that malware had caused a temporary outage. An update in early January clarified that logistics centers and client service activities were impacted by the incident.

The latest statement from Moncler also confirmed a compromise of sensitive personal data. This statement aligns with a DarkCat post on the group's dark web leak site naming and shaming Moncler as a victim of the gang's attacks. Moncler refused to pay the $3 million ransom demand set by BlackCat, which resulted in sensitive data being published online. The published data included customer invoices and earning statements.

Inetum, December 2021

From fashion to IT services, a December 2021 attack on French company Inetum demonstrated the scope of BlackCat's targets. Inetum provides transformative digital services and solutions, including smart agents, computer vision, and AI Ops to businesses around the world.

Inetum is one of the two BlackCat victims for which solid details exist about the attack and its scope. According to a press release on December 23, the attack impacted operations in France but not in any other locations. The scope of the impact was limited, and none of the company's main infrastructures, collaboration tools, or delivery operations were affected.

Interestingly, Inetum didn't disclose BlackCat as responsible for the attack. However, the editor-in-chief of French publication LeMagIt said that the ransomware strain discovered in Inetum's network was authored by BlackCat.

More To Come?

BlackCat is evidently a sophisticated ransomware group. Just as the cybersecurity community thought the ransomware threat might be slowing down, evolutions and innovations promise a new wave of customized attacks that leverage the efficiency and adaptability of the Rust programming language. Generous affiliate offerings are guaranteed to entice more threat actors to sign up with the gang.

Over the course of 2022, expect more attacks to come from BlackCat and more news stories to feature the gang's name. Other new ransomware gangs may form with their own innovations or simply emulate BlackCat's model.

Bringing It Back to Basics

Having the basics of a secure cybersecurity posture in place goes a long way towards dealing with ransomware attacks. Whatever evolutions threat actors come up with in their coding practices, the fact remains that they still need to get initial network access to carry out successful attacks. Preventing initial access requires stopping phishing threats with advanced email security, having multifactor authentication enabled for all critical business apps and services, and ongoing cybersecurity education to ensure good physical and digital security hygiene among employees.

Conti

Conti is a ransomware gang that has managed to wreak havoc on many organizations within just a short time. After first appearing in media headlines as recently as 2019, Conti has been behind several high-profile ransomware incidents. This article analyses Conti's operations, its specific ransomware strain, and several high-profile attacks carried out by the gang that uses Conti.

Conti: Operations and Ransomware Analysis

Similar to REvil, Conti operates a ransomware as a service (RaaS) model. The gang speaks Russian, and it's believed to run operations from St. Petersburg. The slight divergence in Conti's business model from traditional RaaS models is that affiliates using its ransomware strains receive a wage rather than a percentage commission from a successful attack. This operational structure has been confirmed in an advisory published by CISA, the FBI, and NSA.

Rapid encryption and evasive evolution both define Conti ransomware strains. The iterative approach helps the strain become more effective and harder to find over time. Developers can concentrate most of their efforts on updating the ransomware because of the RaaS business model that the gang uses. Initial entry points into networks come from malicious emails, exploiting weak or stolen remote desktop protocol credentials, and targeting common unpatched software vulnerabilities.

The Conti gang doesn't seem to have any concern for its reputation among victims. There have been instances of affected organizations paying ransoms only to not receive encryption keys or not get their data back. The prevailing advice to avoid paying ransoms seems to be particularly pertinent in the case of Conti's ruthless approach.

The gang behind Conti ransomware uses the increasingly popular double extortion technique in its attacks. Not content with just encrypting critical systems, data is first exfiltrated so that victims can't solely depend on a functioning backup and recovery strategy to recover from ransomware. After exfiltrating data, the perpetrators behind Conti ransomware attacks then demand a payment to prevent data from being published on the gang's dark web data leak site.

Data is first exfiltrated so that victims can't solely depend on a functioning backup and recovery strategy to recover from ransomware.

High-Profile Conti Attacks

JVCKenwood: October 2021

The most recent high-profile victim of a Conti ransomware attack was Japanese multinational electronics company JVCKenwood. According to reports, the gang managed to exfiltrate around 1.5 terabytes of data from JVCKenwood's IT network. The exfiltrated data included sensitive information about the company's employees, including phone numbers, contact details, and payroll information.

Conti set its ransom demand at $7 million for this attack. Threat actors used a scanned copy of an employee's passport as proof of the data they exfiltrated from the network. It appears as of the time of writing that JVCKenwood will refuse to cave into the ransom demands set by Conti.

HSE, Ireland: May 2021

In an attack that sent shockwaves across the information security world and the wider general public, Ireland's public health system became the victim of a severe Conti ransomware attack in May 2021. Conducted at the height of Covid-19 with Ireland's fragile health system struggling to cope with hospital surges, the attack on the HSE served as a terrifying example of the gang's ruthless nature.

In an unexpected move, Conti provided a decryption tool to the HSE free of charge a couple of weeks after the attack. Whether this represented some sort of conscience being shown by the gang in light of the global pandemic remains unclear. Even after providing the tool, Conti still demanded ransoms to prevent published confidential health data from being posted online. A full six months after the incident, the knock-on effects were still felt by the HSE.

Broward County Public Schools: March 2021

In another attack exemplifying Conti's intentions to disrupt important public infrastructure and services, Broward County Public Schools in Florida became the latest victim of the gang's operations in March 2021. The ransomware attack resulted in a shutdown of the school district's IT systems.

Negotiations with the perpetrators led to a substantial $40 million ransom demand. Broward County School District refused to pay up, which led to the publication of 26,000 files on the dark web. The published files contained financial and accounting details; however, no personally identifiable student or employee data appears to have been breached.

SEPA, Scotland: December 2019

On Christmas Eve 2019, a BBC news story revealed details of a significant cyber attack on the Scottish Environment Protection Agency (SEPA). The environmental regulator experienced significant disruptions to its core communication systems in the immediate aftermath of the attack. Conti swiftly claimed responsibility for this incident and demanded a ransom payment to decrypt affected systems and return stolen data.

SEPA refused to negotiate on any ransom payment, which led to stolen data being published online less than a month later. The publicly disclosed data included sensitive information about staff and suppliers. The impact on SEPA was such that the regulator's chief executive Terry A'Hearn said it could take a year or two to fully restore all systems.

Defending Against Phishing

By far the most common initial attack vectors in Conti's ransomware attacks are phishing emails. These emails persuade people to download malicious attachments or click links that install remote access software on their devices.

Often, Conti's phishing methods are highly targeted spear-phishing campaigns that leverage information about specific employees found on social platforms such as Twitter and LinkedIn. Using information gleaned about targets, adversaries can write convincing emails that increase the likelihood of being conned.

Employee security awareness training can point out the signs of phishing, but awareness is not enough. Organizations need a dedicated anti-phishing email security solution that can flag and sandbox emails with suspicious links and attachments. Ideally, an email security solution equipped to combat modern phishing campaigns should have AI-driven self-learning capabilities for improved detection.

With an adequate level of defense against phishing, your organization stands a far better chance of thwarting attacks instigated by Conti, or any other ransomware gang.

DarkSide

DarkSide is a ransomware gang that quickly made waves in the cybersecurity world with a range of high-profile attacks. After first notifying the world of their operations in an August 2020 dark web press release, the gang's members have drawn attention by landing some big paydays. This article assesses DarkSide's operations and highlights four high-profile attacks carried out by the gang.

DarkSide: Operations and Ransomware Analysis

Like most of today's most well-known ransomware gangs, DarkSide operates a Ransomware as a Service (RaaS) model in which affiliates that help spread the group's malicious code receive a cut of the commission from any ransom payment. The group's members are believed to be based in Russia

Double extortion is another feature of DarkSide's operations that is shared by several other ransomware gangs. A leak site operates as an outlet for publishing victims' stolen data if they refuse to pay the required ransom. The potential reputational hit from having sensitive customer data published online often serves as the impetus for victims to pay up. This method of extortion pairs with the traditional ransomware extortion in which victims need to pay a sum of money to remove the encryption from affected systems.

The gang targets large companies that can afford substantial payouts. Interestingly, and in contrast to a gang like Conti, DarkSide has publicly announced an unwillingness to target organizations such as hospitals, schools, and non-profits. DarkSide's minor demonstration of something resembling empathy indicates a line drawn by the gang between pursuing profit above all and garnering a worse reputation for targeting vulnerable sectors.

As far as the technical details of DarkSide attacks go, they can be quite sophisticated. Typically, threat actors gain an initial foothold in victims' networks by exploiting remote access technology, such as remote desktop protocol (RDP). This initial foothold starts from either a password compromise enabling log in to a remote access account or by exploiting a vulnerability in the underlying software.

The next phase is command and control using an RDP client routed through the Tor web browser to maintain stealth, as the Tor browser makes it hard to distinguish between malicious and normal web traffic. Using the RDP client, threat actors then seek to move laterally to compromise other hosts, such as servers, especially those lacking detection and response capabilities.

Reconnaissance and credential harvesting are the next steps in the process. Hackers on compromised servers use tools to gather information about users, their credentials, and their privileges. From this information, credential harvesting tools dump password information for user accounts. Privilege escalation comes from hackers using harvested passwords to access administrative accounts.

Data mining and extraction complete the data exfiltration stage while PowerShell scripts delete shadow copies of files so that data can't be restored from those copies. Finally, ransomware payloads are delivered along with unique executables and extensions that evade endpoint antivirus solutions. Victims are met with an ID they can use to access DarkSide's website and make the requested ransom payment.

High-Profile DarkSide Attacks

Colonial Pipeline

The Colonial Pipeline is a 5,500-mile pipeline spanning from its origin in Houston to the Port of New York and New Jersey. The pipeline's operator, Colonial Pipeline Company, earned $1.3 billion in 2020 alone.

In May 2021, DarkSide set the pipeline in its sights and managed to infiltrate |Colonial Pipeline's IT network using VPN account credentials stolen in a previous data breach. What followed was one of 2021's biggest cybersecurity stories. Colonial Pipeline engaged in emergency procedures to contain the attack, which meant shutting down the normal operations that ensure a smooth supply of gasoline, diesel, and jet fuel.

After six days of operational disruption and a degree of chaos at filling stations, the pipeline resumed normal operations. DarkSide received a ransom payment in Bitcoin worth $4.4 million. The FBI has since helped to partially recover $2.3 million worth of Bitcoin by obtaining the private key for the gang's ransom account.

CompuCom

CompuCom is a US-based technology company that provides end-to-end managed services. CompuCom was acquired for $1 billion in 2017 by Office Depot. In March 2021, the company became the latest victim of a DarkSide ransomware attack that impacted its service delivery for up to 16 days.

Details remain sketchy about the initial infiltration of CompuCom's network. However, a company FAQ about the incident confirmed the use of Cobalt Strike, a common penetration testing tool, to conduct stealthy command and control operations.

CompuCom estimated the total cost of this attack at $28 million. These costs include lost revenue of between $5 million and $8 million due to service disruptions.

Toshiba Tec Group

Toshiba Tec Corp is a strong-performing business unit belonging to the Japanese multinational conglomerate with a $2.3 billion valuation. This incident went a little bit under the radar because it happened right around the time of the Colonial Pipeline attack.

An official company comment mentioned that the extent of the attack was limited to some European regions. Containment and backup measures were enacted to limit the ability of the ransomware to spread. A Reuters report indicated that the threat actors managed to exfiltrate up to 740 gigabytes of data, some of which was sensitive.

Coinciding with the Colonial Pipeline incident, the targeting of two high-revenue organizations so close in time to each other demonstrates the scale of DarkSide's operations. One senior malware analyst pointed out that, "there are around 30 groups within DarkSide that are attempting to hack companies all the time".

The Future of DarkSide

The governmental intervention and skyrocketing publicity brought about by the Colonial Pipeline attack led to the gang's May 2021 announcement that it was ceasing operations. The heat from law enforcement resulted in an unnamed government seizing the group's servers and other infrastructure.

As is often the case, the spotlight from law enforcement doesn't necessarily mean the end of a ransomware gang's operations. A new operation named BlackMatter emerged just under two months later carrying the hallmarks of DarkSide's encryption methods. This unique encryption algorithm was not widely used by other ransomware gangs.

Security researchers also speculate that the similarities in the color palette and language used on the BlackMatter website further identify this new operation as a rebranding of DarkSide. It's worth keeping an eye on future cyber attacks conducted by BlackMatter to see whether the victim profile also matches that of DarkSide.

Tips for Preventing DarkSide Attacks

The following actions can help to prevent your organization from becoming the next victim of a ransomware gang like DarkSide:

Deploy an API-based email security solution to detect and remediate advanced phishing attacks

Avoid exposing ports to the public Internet for remote desktop connections

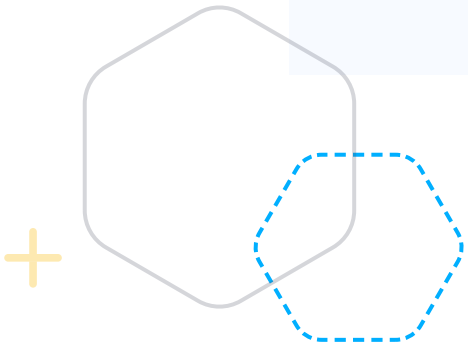
For anyone connecting to the network using remote access technology, put multifactor authentication in place so that hacking passwords isn't enough to gain a foothold

Have a lockout policy in place that locks users out from their remote access or VPN accounts after a certain number of incorrect password attempts

Establish a patch management policy that ensures all software and operating systems are kept up to date with the latest security fixes

Get comprehensive endpoint detection and response across your entire endpoint inventory; not just some of your endpoints

Regularly back up important data and store this data in an isolated location offline and disconnected from your network



REvil

REvil is a notorious ransomware gang responsible for multiple high-profile cyber attacks targeting companies of all sizes. This article explores REvil's origins, the types of malware payloads used by REvil, and some of the most infamous attacks featuring the gang's malware variants.

REvil: A Brief Background

REvil (Ransomware Evil) is a private group that runs a ransomware-as-a-service operation. The service model of ransomware works as follows:

- The gang's developers create one or more functioning ransomware variants.
- The gang makes these ransomware variants available to paying customers—threat actors seeking to compromise organizations—for some form of payment.
- The type of payment can be a monthly subscription fee or an affiliate model in which the gang receives a percentage of any ransom payments received by customers.
- The developers focus most of their efforts on creating more effective ransomware strains.
- A typical service offering comes bundled with other features, such as 24/7 support, to further attract customers.

REvil's members speak Russian and are likely to be Russian citizens. In 2019, security researcher Brian Krebs speculated that REvil was a probable rebranding by a group formerly known as GandCrab. Subsequent investigations have found t hat both REvil and GandCrab ransomware operations were run by the Russian-based group PINCHY SPIDER.

REvil Malware Analysis

The execution of ransomware strains on multiple machines is the final phase of a complex chain of events that starts with infiltrating a network. The payload used to carry out ransomware attacks involving REvil is known as Sodinokibi (Ransom. Sodinokibi). This payload encrypts multiple local files on the affected system and displays a ransomware note demanding payment to remove the encryption.

Sodinokibi malware has inbuilt features that help it evade detection, such as deleting the virus definition database used by Windows Defender. The malware uses a complex combination of symmetric and asymmetric encryption to lock down files. Ransom demands appear on the desktop background of infected systems with instructions to make payment using Monero cryptocurrency. Monero has additional privacy features, such as hidden addresses, that other cryptocurrencies lack, which makes payments much harder to trace.

High-Profile REvil Attacks

Security researchers and investigators believe that hundreds of companies have been victims of REvil ransomware strains. Here are four of the most high-profile incidents that exemplify the scale of REvil's operations.

Travelex, January 2020

Foreign currency exchange and travel insurance company Travelex became one of the earliest high-profile casualties of REvil ransomware. The attack exploited security vulnerabilities in Pulse Secure, which is a corporate VPN application that facilitates remote connections to the network. Travelex paid a ransom of at least $2.3 million in the aftermath of the attack, and the financial impacts of dealing with the attack resulted in the company going into administration with the loss of 1,300 UK jobs.

From a security perspective, the mistakes made by Travelex were particularly shocking given that patches were available for the exploited vulnerabilities well over four months before the attack. Up to seven Pulse Secure VPN servers remained unpatched, which allowed threat actors to gain access without a username or password. From this initial access point, moving laterally through the network, the intruders installed REvil's Sodinokibi ransomware strain.

Grubman Shire Meiselas & Sacks, May 2020

Another high-profile incident bearing the name of REvil was a May 2020 ransomware attack on law firm Grubman Shire Meiselas & Sacks. The law firm focuses on the media and entertainment sector, and the clients on its books include names such as Rod Stewart, Madonna, and Lady Gaga. In the attack, REvil managed to exfiltrate 756 gigabytes of private documents and correspondence from GSMS' network.

REvil claimed responsibility for this attack on the dark web and demanded a payment of up to $21 million. REvil also attempted to auction stolen information about Bruce Springsteen on the dark web to the highest bidder, however, no bidders came forward. GSMS ultimately chose not to pay the ransom.

JBS, June 2021

JBS, the world's largest meat supplier, became the victim of REvil's ransomware operations in June 2021. The attack on JBS resulted in operational disruptions at slaughterhouses in the United States and Australia. Data exfiltration, in which threat actors first steal data from systems before installing ransomware, was a prominent aspect of this incident.

The JBS attack was particularly profitable for REvil. The victim paid a substantial $11 million worth of Bitcoin to decrypt systems and resume operations. The consensus among national bodies is that victims should avoid paying ransoms because such payments could incentivize future attacks. It's clear that for JBS, resuming critical business operations took precedence over listening to the recommended advice.

Kaseya, July 2021

The attack on US IT software provider Kaseya in July 2021 made headlines around the world due to the vast scale of its impact. The Kaseya incident targeted Kaseya VSA, which is a remote computer management tool used by organizations and managed IT providers. Kaseya VSA had critical security flaws that threat actors were able to exploit.

This attack resulted in the compromise and encryption of thousands of systems belonging to well over 1,500 different businesses. The distinguishing feature that clearly identified REvil's role in the attack was the malicious Sodinokibi payload. Arguably the most memorable outcome of the Kaseya attack was the news that Swedish grocery chain Coop had to close 800 stores because point of sale (POS) systems stopped functioning.

The Future of REvil

On July 13, 2021, in what was still the fallout of the Kaseya attack, REvil's dark web ransomware website and blog went offline. Rumors continue to circulate in the security community and beyond about exactly what happened to REvil. The general consensus is that authorities in either the United States or Russia tracked REvil and forced the gang to cease operations.

Mounting tension between the United States and Russia over cyber incidents originating in Russia makes it arguably more likely that the Russian government forced REvil offline in an effort to ease those tensions. Whatever the truth, it appears REvil's members and customers drew too much attention to themselves by conducting large-scale attacks that drew widespread media publicity.

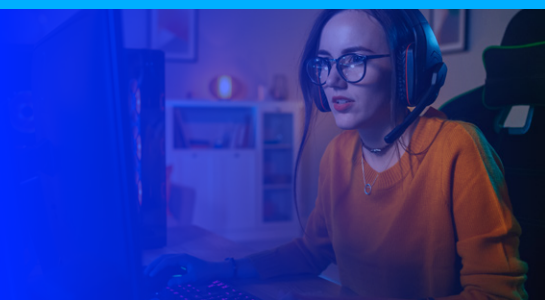
In bad news for both authorities and businesses around the world trying to prevent and defend against cyber attacks, REvil resurfaced in September 2021. The gang's blog, other connected websites, and infrastructure were back online by September 8. It seems a matter of time before the next attack involving REvil comes to light.

Preventing Initial Network Intrusions

The initial intrusion into a network is the start of all ransomware attacks. Compromised credentials obtained through phishing attacks often provide an entry point into applications and systems. Here are some tips to prevent network intrusions and ensure groups like REvil can't install ransomware strains on your network:

- **Combat against the threat of phishing emails** with an anti-phishing email security solution that blocks these deceptive emails from reaching users and convincing them to give up their passwords or download malicious files.
- **Consider using non-standard ports for services** such as RDP that threat actors regularly try to break into.
- **Use multifactor authentication for business services** and applications so that even if hackers manage to guess, obtain, or steal the right password, they can't get into a targeted system without an additional piece of evidence.
- **Regularly remind employees and users about the importance of good password hygiene**, which means using longer passwords that combine upper and lower cases with symbols while avoiding reusing passwords across multiple apps and services.

Ragnarok



Ragnarok is a ransomware gang known for the Ragnar Locker ransomware, which has impacted a range of high-profile organizations from video game developers to energy companies. This article looks at Ragnarok's operations, ransomware strain, and some high-profile attacks carried out by the gang.

Ragnarok: Operations and Ransomware Analysis

Ragnarok uses classic double extortion tactics to first exfiltrate data from enterprise IT systems before locking down files, servers, and workstations. Attacks often begin by exploiting weak or stolen passwords used to log in to RDP services. Lateral movement comes from exploiting vulnerabilities, such as CVE-2017-0213, to elevate privileges.

After escalating privileges within compromised networks, threat actors install the ransomware strain and delete volume shadow copies; the latter step prevents administrators from recovering files using older, encrypted versions. Alongside these pretty standard ransomware operations and tactics, Ragnarok has some peculiarities worth mentioning.

An intriguing tactic uncovered by security researchers is that the Ragnarok gang uses virtual machines installed on compromised systems and runs its ransomware inside those VMs. This is a stealth tactic designed to bypass endpoint security solutions that may detect the ransomware. Any changes made to system files appear to come from legitimate VM software so that anti-malware solutions don't flag the activity as suspicious.

Many ransomware strains try to evade detection by listing and killing currently running local processes, such as antivirus solutions. The use of VMs serves as another example of the creativity threat actors increasingly demonstrate in ensuring their ransomware attacks have the best chances of succeeding. Given the short shelf-life of many ransomware strains and gangs today, this evolution in tactics is arguably what should capture the most attention about Ragnarok from a security perspective.

From an operational perspective, Ragnarok further garnered media attention by warning victims not to contact law enforcement. In an announcement post published on Ragnarok's dark web leak site, the gang threatens that "if you hire any recovery company for negotiations or if you will send requests to the police/FBI/investigators, we will consider this as a hostile intent and we will initiate the publication of whole compromised data immediately."

This operational tweak perhaps reflects a degree of panic among the gang's members. After noting how law enforcement quickly closed in and managed to shut down several high-profile ransomware operations in mid-2021, Ragnarok probably feared the same fate.

Ragnar Locker Victims

Within a relatively short timeframe, Ragnarok threat actors managed to infiltrate the networks of several high-profile victims, steal their data, and encrypt important files.

Energias de Portugal (EDP), April 2020

An attack on Portuguese electric utility company EDP marked the first publicly disclosed, high-profile incident involving the Ragnar Locker ransomware. A letter sent to customers of the North American branch of EDP outlined how the company's parent corporation, "experienced a ransomware attack on its information systems...the attackers had gained unauthorized access to at least some information stored on the company's own information systems."

The ransom note left by Ragnarok demanded a payment in Bitcoin equating to $10 million at the time. The gang's member told EDP that they managed to exfiltrate up to 10 terabytes of data from its IT infrastructure. Remediation efforts attempted to limit the reputational impact by offering affected EDP customers one free year of identity protection services.

Campari Group, November 2020

Marking the start of a month in which Ragnarok managed to attack at least two high-profile victims, Campari Group revealed a severe ransomware attack that infiltrated the Italian liqueur makers' IT systems in early November 2020. The company, which makes a signature liqueur known to customers globally, generated revenues just short of €1.8 billion in 2020.

Reports suggested the Ragnar Locker ransomware encrypted Campari Group IT servers in up to 24 different locations. Demands for a substantial $15 million ransom indicated high levels of sensitive data exposure and/or a severe compromise in IT infrastructure. Subsequent technical investigations revealed compromises of some sensitive personal and business data, including names, surnames, e-mail addresses, and mobile phone numbers for over 4,000 employees.

Capcom, November 2020

A second high-profile ransomware attack in November 2020 by Ragnarok's threat actors resulted in what video game developer Capcom described as a customized ransomware attack on its systems. The Japanese company is particularly well-known for the Resident Evil series of zombie-based video games with combined sales of over 120 million copies.

A company statement outlined an extensive list of potentially compromised data that included personally identifiable information in up to 350,000 items. Investigations revealed the initial entry point came from compromised credentials for an old backup VPN account.

ADATA, May 2021

ADATA is a Taiwanese computer storage and memory manufacturer that counts Solid State Drives, external storage (HDD, SSD, Enclosures, and USB flash drives among its main consumer-focused products. ADATA's accounts showed revenues close to $1 billion in 2019, and the company has over 1,400 employees.

Near the end of May 2021, Ragnarok threat actors infiltrated ADATA's network and installed the Ragnar Locker ransomware strain on multiple systems. According to gang members, they managed to steal up to 1.5 terabytes of sensitive information before installing ransomware. ADATA managed to act quickly to bring affected systems offline before the ransomware propagated further through the company's network.

Ragnarok: Disbandment and Future

In August 2021, Ragnarok announced an abrupt shutdown of its operations. Threat actors even released the decryption key for all victims to fully restore any remaining encrypted files or systems.

It is interesting to speculate whether this sudden disbandment reflected pressure from law enforcement. This would be somewhat ironic considering the gang's assertion that any victim contacting the law would have their data published openly to the world.

Another angle on the gang's departure is that perhaps one or more victim organizations caved into ransom demands, which led to a large payday and early retirement for gang members. Whether or not these threat actors re-emerge with a new version of Ragnar Locker remains to be seen. It's not unheard of for a ransomware gang to announce an operational shutdown before coming back on the radar a few months later.

Credential Phishing

A clear pattern emerging through Ragnarok's attacks is the exploitation of relatively obvious vulnerabilities to gain initial network access. Stolen or compromised credentials for VPNs, RDP, and other systems are a common network entry point. Threat actors get their hands on passwords from brute force guessing easy passwords, reusing passwords from other leaks published to the dark web, or from credential phishing.

Credential phishing attacks use psychological tactics, including eliciting urgency or exploiting familiarity, to get targets to click malicious links and enter their login credentials on fake login pages that appear genuine. Often, these emails come from spoofed email addresses that look like they come from brand name companies.

Some credential phishing attacks point to malicious web pages that contain images rather than login forms. Targets enter their passwords into the image without knowing its malicious intent. Adversaries perform this tactic in an attempt to avoid flagging filters that may block suspicious URLs based on the fact they contain login forms.

To adequately combat credential phishing, organizations need an email security solution that leverages machine learning advancements to detect and block credential phishing attacks. A self-learning solution ensures the blocking component of the solution improves over time by looking for emails that were incorrectly allowed to enter inboxes without any flagging or blocking. The reinforced learning paradigm helps solutions leverage real-world data to quickly become extremely accurate at blocking any potential phishing email.

Closing Thoughts

Ransomware gangs will come and go, but the threat will always be present. Companies need to treat ransomware as a high-risk incident that they are exposed to at all times. Recovery can be incredibly painful, so it's best to get in place the right mindset, tools, and processes to prevent ransomware before it can cause damage.

To learn more about IRONSCALES' award-winning anti-phishing solution, please sign up for a demo today

IRONSCALES
SAFER TOGETHER

IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks and launched globally. Legacy technologies like security email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

To learn more, please visit **www.ironscales.com** today!