Netwalker Ransomware Guide: Everything You Need to Know

By Nathan Coppinger

Published: 2020-11-17 · Archived: 2026-04-05 16:40:55 UTC

Emotet, Trickbot, Maze, Ryuk, and now Netwalker ransomware— cybercrime has increased exponentially in the last year. Ransomware has been a serious plight across industries big and small, public and private, with no sign of letting up.

In 2019 alone, attackers extorted an estimated $11.5 billion from their victims, up from $8B in 2018. Experts estimate that the cost of ransomware attacks will increase by nearly 100% to $20B by 2021. Netwalker (aka Mailto) has cashed in over $30M in ransoms since their first significant attacks in March.

Get a Free Data Risk Assessment

What is Netwalker Ransomware?

The Netwalker ransomware is a fast-growing ransomware, created by the cybercrime group known as 'Circus Spider' in 2019. Circus Spider is one of the newer members of the 'Mummy Spider' cybercriminal group. On the surface, Netwalker acts like most other ransomware variants, establishing an initial foothold through phishing emails, followed by exfiltrating and encrypting sensitive data to hold hostage for a large ransom.

Unfortunately, Netwalker does more than hold the victims' data hostage. To show they are serious, Circus Spider will leak a sample of the stolen data online, claiming that if the victim does not meet their demands in time, they will release the rest on the dark web. Circus Spider leaked one victim's sensitive data onto the dark web in a password-protected folder and published the key online.

Netwalker Ransomware Adopts a RaaS Model

In March of 2020, Circus Spider decided that they wanted Netwalker to become a household name, so they decided to expand their affiliate network, much like the Maze ransomware gang. Shifting to a ransomware-as-a-service (RaaS) model allowed them to operate on a much larger scale, target more organizations, and increase the size of their ransoms.

RaaS involves recruiting affiliates to help cybercriminal groups execute nefarious activities. As mentioned above, Netwalker started gaining momentum with a few big scores. However, they were still relatively small compared to the other big-time ransomware gangs… *until* they adopted a RaaS model.

To gain the (dis)honor of joining their small band of criminals, Circus Spider posted a specific set of criteria required, or a criminal job posting if you please.

Their main criteria for affiliates consist of:

- Experience in networks

- Speaks Russian (specifically, they do not accept English speakers)
- They will not train inexperienced users
- Consistent access to quality targets
- Proof of experience

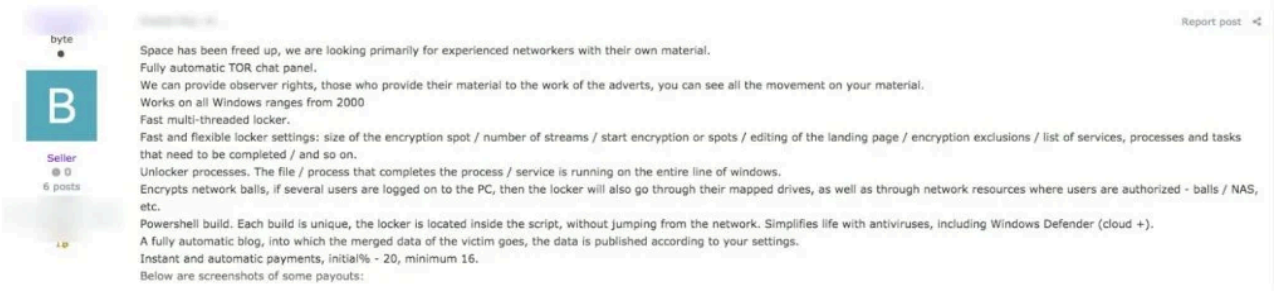
> The Sodinokibi/REvil ransomware gang is looking for partners specialized in network attacks pic.twitter.com/m3lYN5qk8t
>
> — Catalin Cimpanu (@campuscodi) April 19, 2020

> …and now, the Netwalker (Mailto) ransomware gang is also looking for two partners specialized in network attacks
>
> Trend for ransomware attacks/intrusions is pretty obvious these days. Gangs moving away from spear-phishing to targeting internet-exposed RDPs and servers. pic.twitter.com/VKWl9Q0vaa
>
> — Catalin Cimpanu (@campuscodi) April 29, 2020

To attract the best prospects possible, Circus Spider published a list of features that their new partners, if chosen, will be granted access to.

These include:

- Fully automatic TOR chat Panel
- Observer rights
- Works on all Windows devices from windows 2000 up
- Fast multi-thread locker
- Fast and flexible locker settings
- Unlocker processes
- Adjacent network encryption
- Unique PowerShell builds making it easier to deal with antivirus software
- Instant payouts



Who and What Does Netwalker Ransomware Target?

Since their first big score in March, there has been an uptick in Netwalker ransomware attacks, primarily targeting healthcare and education institutions. They carried out one of their more publicized against a large university that specializes in medical research. This university had their sensitive data stolen by the ransomware, and to show that

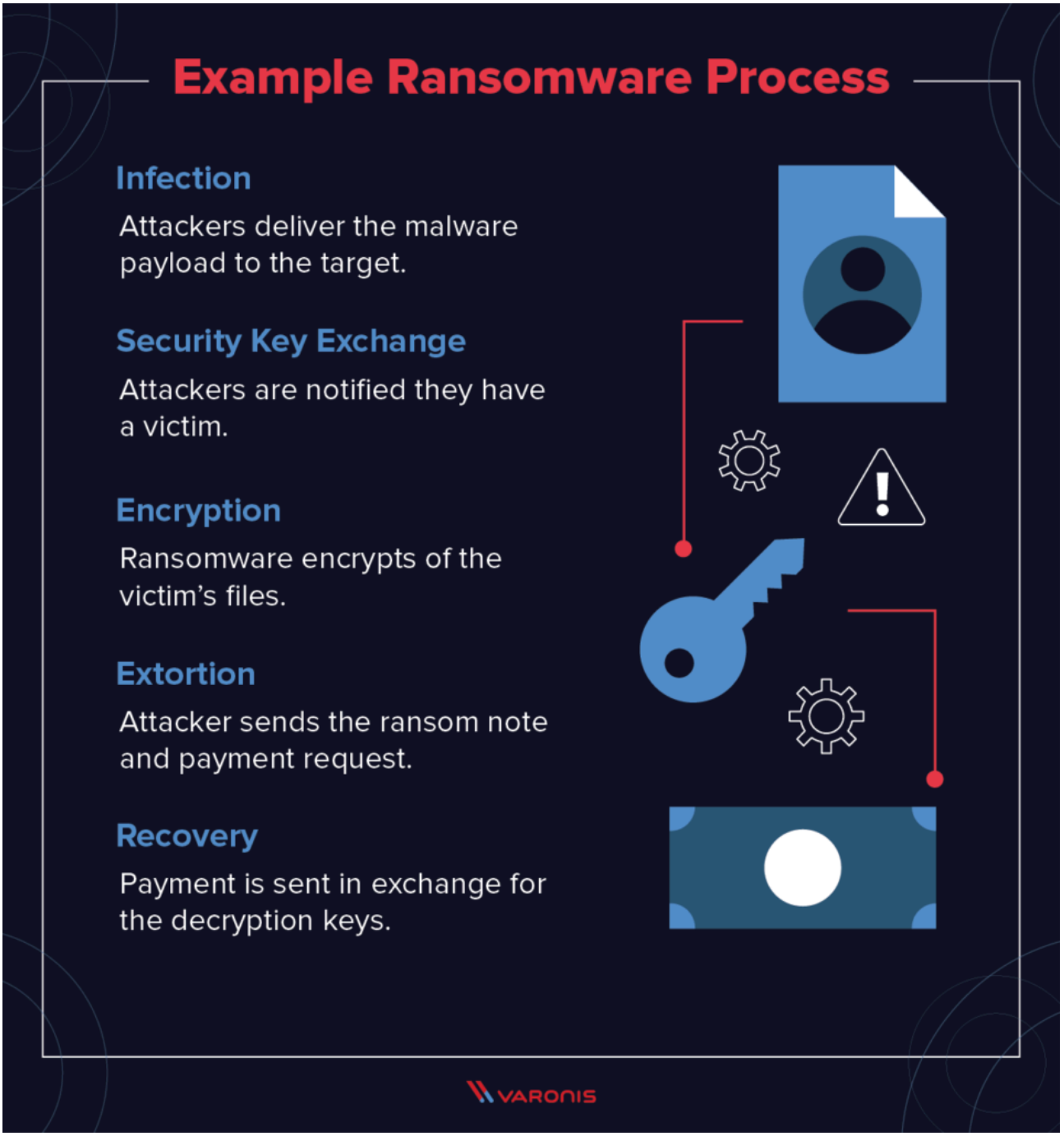
they weren't playing around, the attackers leaked a sample of the data they had stolen. This data included student applications containing information such as social security numbers and other sensitive data. This breach led to the victim paying their attackers a $1.14M ransom to decrypt their data.

There has been a big push by Netwalker attackers to capitalize on the chaos of COVID-19 by sending out pandemic-related phishing emails and targeting healthcare institutions that are already overwhelmed by the pandemic. One of the first healthcare victims had their site taken down by the ransomware just as the public began to turn to them for advice during the pandemic. This attack forced them to launch a second site and route users to the new one, causing distress and confusion for everyone involved. As the year went on, Netwalker and other ransomware groups continued to target healthcare institutions, particularly because they tend to have understaffed IT departments and are focused more heavily on other areas of their organizations.

In addition to healthcare and education, Netwalker targets various other industries including:

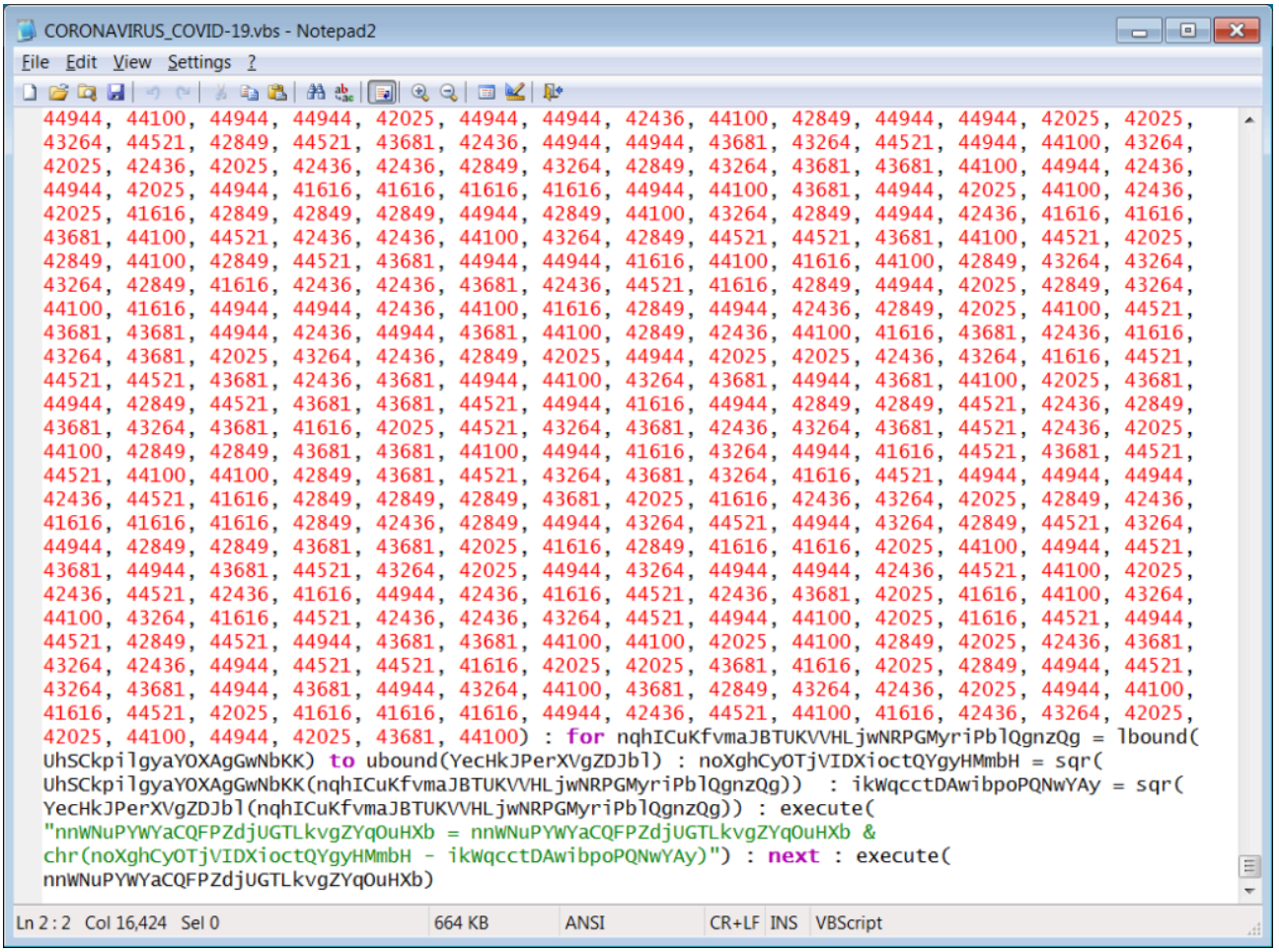
- Manufacturing
- Business management solutions
- Customer experience management
- Electromobility and battery solutions
- Education
- And many more

How Does Netwalker Work?



Step 1: Phishing and Infiltration

Netwalker relies heavily on phishing and spear-phishing as their method of infiltration. As per the norm of phishing campaigns, Netwalker will often send out emails that appear like they were sent from legitimate sources to trap victims in their web. Commonly Netwalker will attach a VBS script named "CORONAVIRUS_COVID-19.vbs" that will execute the ransomware when they double-click the email or open the attached word document that contains the malicious script.



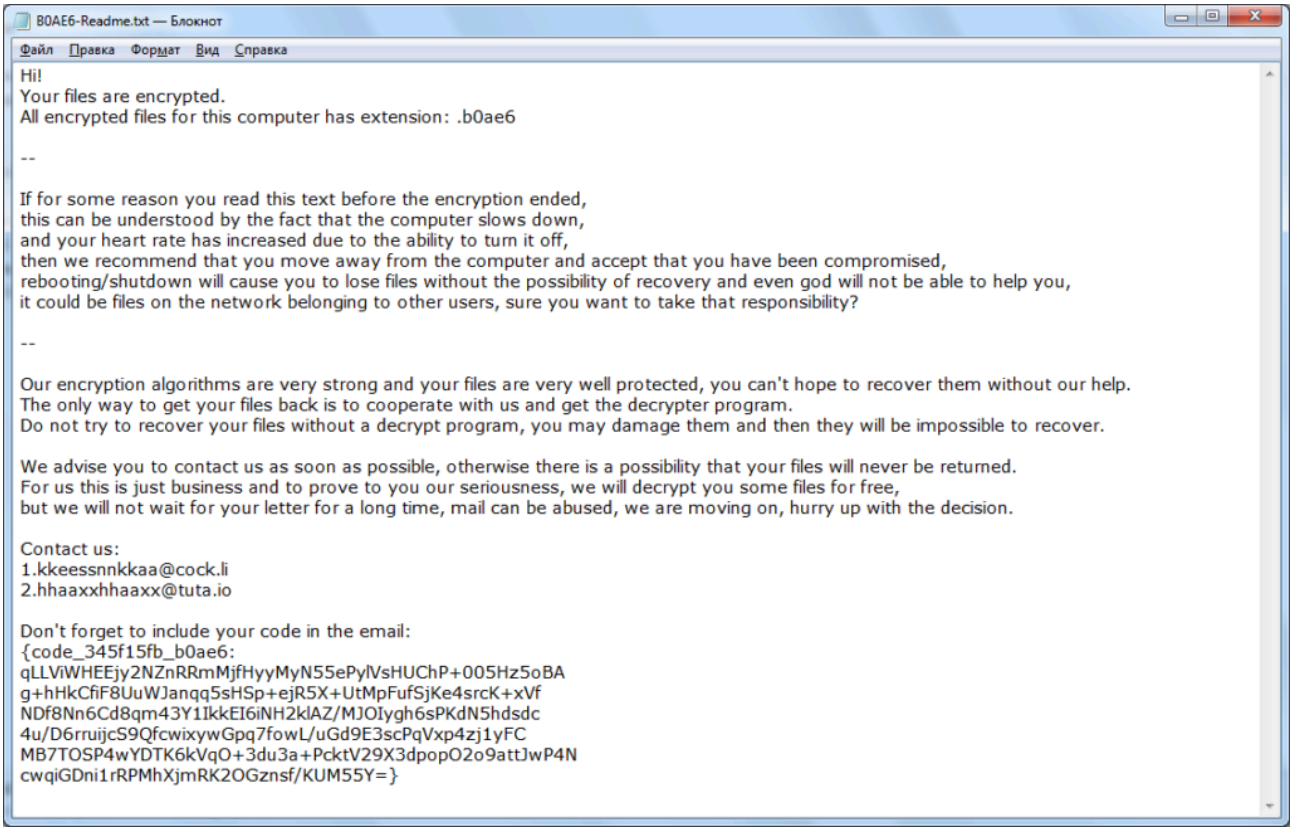
(VBS Script)

Step 2: Data Exfiltration and Encryption

If the script opens and runs on your system, then Netwalker has officially begun to burrow into your network, and the countdown to encryption begins. Once in your system, the ransomware will morph into a legitimate-looking process, usually in the form of a Microsoft executable. It achieves this by removing the code from an executable and injecting its own malicious code into it to access process.exe. This method is known as process hollowing. Process hollowing gives the ransomware plenty of time to work its way through the network unseen— exfiltrating and encrypting data, deleting back-ups, and leaving backdoors before anyone notices anything is wrong.

Step 3: Data Extortion and Recovery (or Loss)

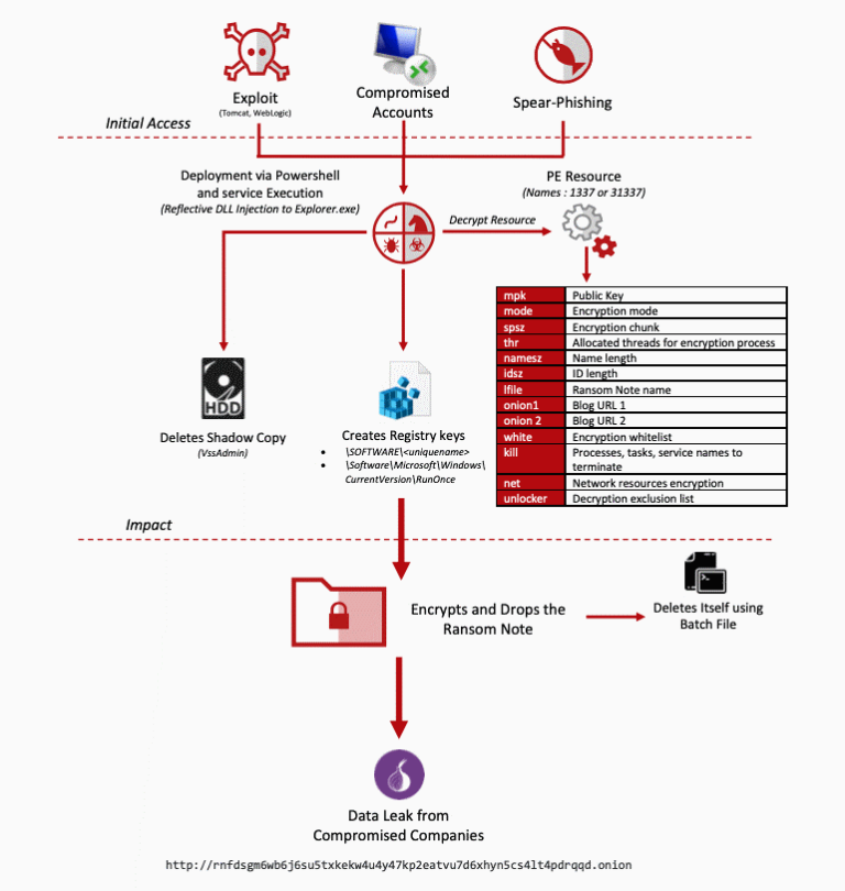
Once Netwalker has finished exfiltrating and encrypting data, the victim will have noticed something is terribly wrong and find the dreaded ransom note. Netwalker's ransom note is relatively standard, laying out what has just occurred and what needs to happen next if the user wants their data returned safely. Circus Spider will then demand a set amount of money to be paid in Bitcoins, using a TOR browser portal.



(Source)

Once their victims meet their demands, they grant them access to their custom decryption tool to safely decrypt their data. Circus Spider will increase their ransom and/or release some of or all the stolen data onto the dark web if they do not meet their demands in time.

Below is a diagram of Netwalker's specific attack path



(source)

Tips on Protecting Yourself From Netwalker Ransomware

Netwalker continues to become more sophisticated and harder to defend against, mainly as they grow their affiliate network, and it is imperative to take steps to protect yourself. Netwalker has done enough damage to catch the U.S. government's eye, and the FBI's cybercrime division released a Flash warning, TLP: White, advising organizations to be on the lookout for malicious phishing emails related to the pandemic.

The FBI has recommended the following mitigation procedures:

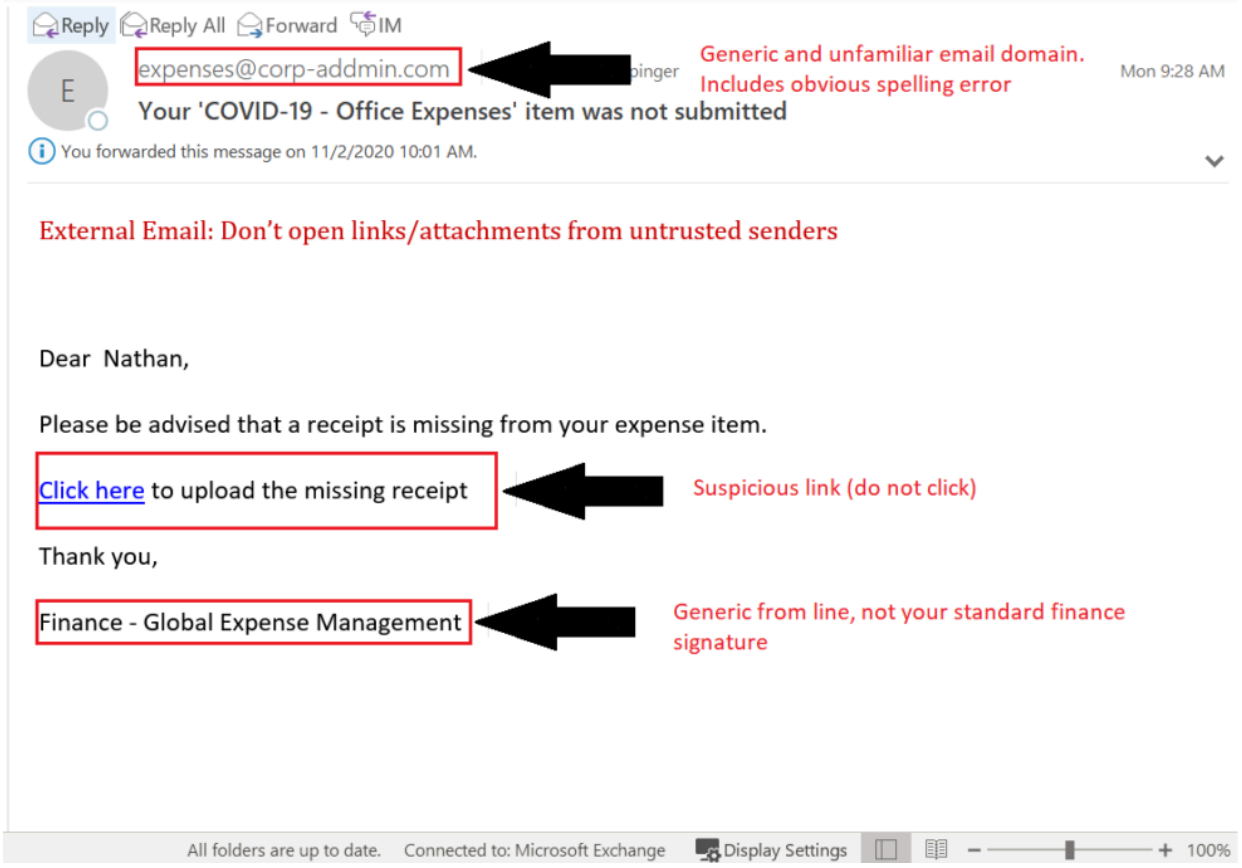
- Back-up critical data offline.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
- Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.
- Install and regularly update anti-virus or anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Use two-factor authentication with strong passwords.
- Keep computers, devices, and applications patched and up to date. Netwalker, like other ransomware, takes advantage of vulnerabilities in your systems and infrastructure to take control of the users' computers and entire networks and holds your data hostage until you pay their ransom.

While these procedures will help mitigate the damage done by the ransomware once it has infected your system, it is still just that, mitigation. Proactively performing these procedures will help prevent the spread and reduce the ransomware's damage once it has infiltrated your system. But prevention education will be a powerful weapon in the war against Netwalker.

Don't Get Caught on This Phishing Trip

Because Netwalker mainly uses phishing attacks with malicious links and executables to infect systems, educating your organization on the dangers of phishing campaigns and what to look for to filter out suspicious emails is imperative to the safety and protection of your sensitive data. Requiring regular data security training is an excellent prevention method and helps your organization learn the signs of malicious emails. Here are some things to check anytime you receive an email asking you to click a link, download a file, or share your credentials.

- Double-check the name and domain the email is from
- Check for obvious spelling errors in the subject and body
- Do not share credentials—legitimate senders will never ask for them
- Do not open any attachments or download any suspicious links
- Report suspicious emails to whoever handles your IT security



To ensure that your social engineering education made an impact on your security measures, we also recommend running attack simulations. Sending out fake phishing emails to your organization is a great way to gauge your security training's success and pinpoint who might need a little extra help in the matter. Track metrics on user

interactions to see who interacts with any of the links or attachments, gives out their credentials or, reports it to your organization's proper authorities.

How Varonis Can Help

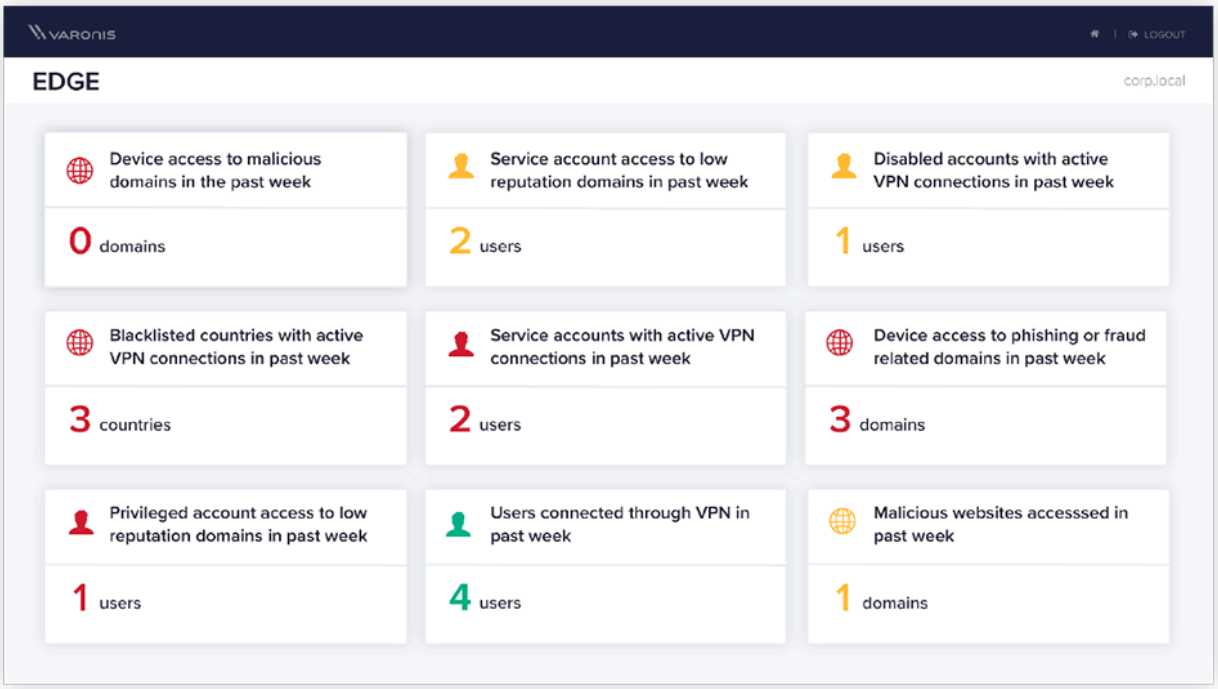
Educating your organization on ransomware-related phishing attacks is a great help in protecting your sensitive data. But taking your defenses a step further with proactive threat detection and data security can limit your exposure to damaging consequences even further.

Protect Yourself with Behavior-Based Threat Detection

Varonis can alert you to early signs of compromise by ransomware gangs with behavior-based threat models for each phase of the kill chain. We build users' profiles across multiple platforms, combining subtle deviations in email behavior with suspicious logon events, network connections, and data access. These unique combinations help us catch threats other security solutions miss and result in few false positives.

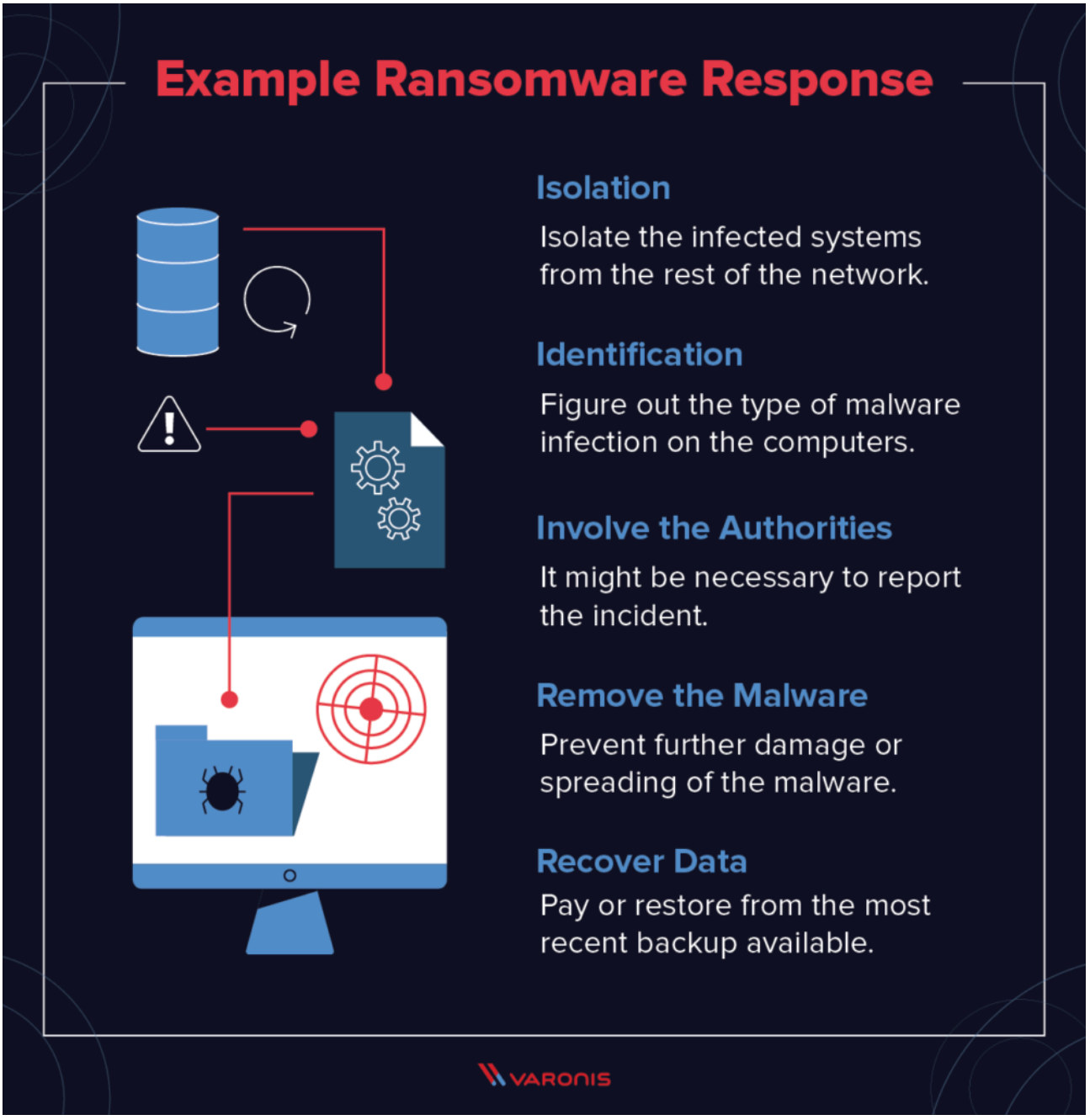
Varonis can detect phishing attempts by monitoring Microsoft Exchange and Exchange Online mailboxes for malicious file attachments that match a dictionary of known patterns used in standard ransomware spam templates.

With Edge's proxy-based detections, customers can also detect when a user downloads an attachment or clicks on a link within the body of an email that results in a malicious Netwalker loader download.



If a compromised user account begins accessing sensitive data, Varonis' behavior-based threat detection will be on top of it. Varonis uses multiple behavior models to learn how specific users access data regularly and can detect when that user starts to access an unusual amount of data compared to their normal behavior. Varonis can differentiate between manual and automated actions and catch if a user begins to exfiltrate and encrypt files in an abnormal manner, stopping the ransomware in its tracks. Many customers automate responses to this kind of behavior, disabling the account, and killing active connections.

By watching file system activity, Varonis quickly detects when ransomware saves known penetration tools to disk (a common Netwalker tactic), or when a user searches file shares for files containing passwords or other sensitive data. Any given user account typically has access to far more data than they should, so these searches are frequently fruitful – more on mitigating this below.



Get to Least Privilege and Reduce Your Attack Surface

Having the right detection in place is a crucial step toward protecting your organization from ransomware. Equally important, however, is ensuring that if ransomware does evade initial detection, its impact is minimal. Organizations can do this by minimizing the data they have exposed, thereby limiting the data that can be encrypted or stolen. Varonis reveals where data is overly accessible and automates processes to lock it down so you can not only limit your attack surface but also limit the damage a ransomware infection can do.

Stay Alert and on Top of Things… Time is of The Essence

If you suspect that you have been a victim of the Netwalker Ransomware, act quickly. Run a query for all the file accesses and modifications made by any user over any period of time to pinpoint affected files and restore the

correct versions. You can also call on our world-class Incident Response Team for help investigating an incident for free.

Harden Your Defenses– Get a Free Ransomware Preparedness Assessment

Ransomware has become more sophisticated and harder to detect. Organizations need to proactively limit their attack surface and put in place effective detection methods to stay ahead. Varonis has extensive experience in detecting and preventing ransomware infections. To see where you might be vulnerable and gauge your readiness for a potential attack, sign up for a free ransomware preparedness assessment. We'll provide you with a detailed report customized to your environment and can discuss remediation steps you can take to better protect your organization from a damaging attack.
