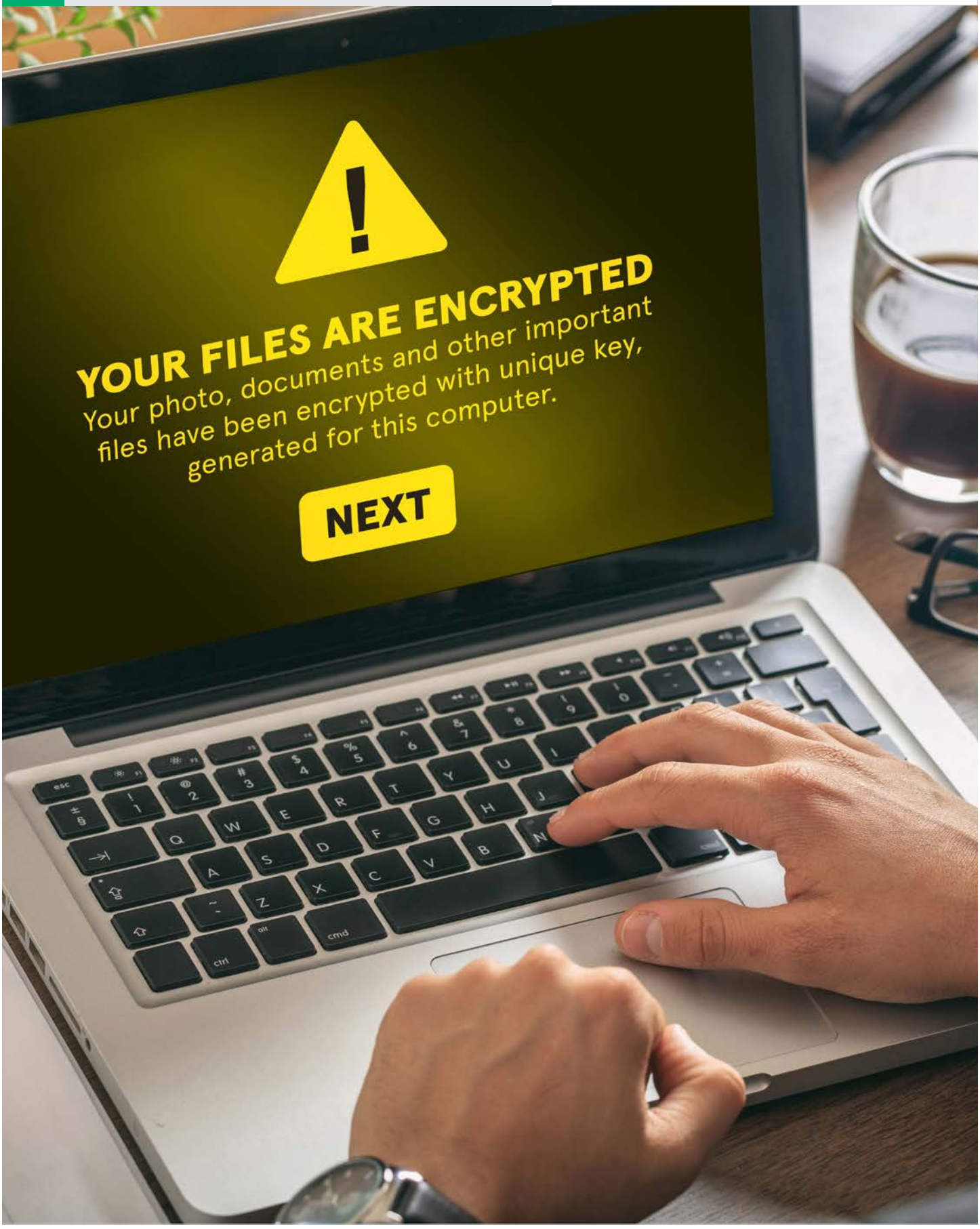
Ransom(*Every*)Ware

Lessons Learned on the Front Lines of Record-Breaking Ransomware Attacks

neustar®

www.home.neustar

Table of Contents


YOUR FILES ARE ENCRYPTED
Your photo, documents and other important files have been encrypted with unique key, generated for this computer.
NEXT

Ransomware Is Everyware

Believe it or not, ransomware is not new. The notion of breaking into, infecting, and holding a network hostage dates back to 1989, when an attacker distributed 20,000 infected and malicious diskettes to attendees at a conference[1]. Despite occurring almost 30 years ago, ransomware never entered the public lexicon – until recently.

In May of 2017, the world was introduced to WannaCry, a potent strain of ransomware code that infected and paralyzed 230,000 computers across 150 countries. Unlike other cyberattacks, it didn't force down the front door with a crushing distributed denial of service (DDoS) attack. And it didn't poke and probe repeatedly until it found a chink in the security armor. Instead, WannaCry quietly targeted an obscure vulnerability in outdated Microsoft Windows operating systems.

In what would become a troubling theme, WannaCry, and subsequent strains of ransomware, could have been prevented from becoming a public nuisance had proper maintenance and diligence been employed. But it was too late; Pandora's box was now open. A month later computers in more than 65 countries were hit by Petya and NotPetya ransomware, which again targeted a patchable software vulnerability.

These were just the beginning of a surge of ransomware attacks around the world that has never slowed – and has increasingly focused on businesses as the target. In 2018, about 70% of ransomware attacks targeted businesses,[2] a number that soared by 195% in the first quarter of 2019.[3] By 2020, ransomware had become the most observed threat, affecting more than 62% of organizations with costs estimated to add up to a staggering $20 billion worldwide.[4]

For enterprise security teams, the message is clear: ransomware is everywhere.

1 http://www.csoonline.com/article/3095956/data-breach/the-history-of-ransomware.html#slide2
2 https://healthitsecurity.com/news/71-of-ransomware-attacks-targeted-small-businesses-in-2018
3 https://healthitsecurity.com/news/ransomware-attacks-on-business-targets-increase-by-195-in-q1
4 2020 Cyberthreat Defense Report, CyberEdge Group

What Is Ransomware, Anyway?

Ransomware has become the poster child for what security experts refer to as an evolving threat landscape. It emerged as a global threat only when cybercrooks needed a new money-making scheme; because so much stolen data was up for sale on the black market... prices for it fell. The trend has continued evolving ever since.

Sophisticated crooks now offer ransomware-as-a-service; GandCrab reportedly cleared USD $2 billion for its affiliated cybercriminals[5]. Expanded attack vectors include malicious emails, batch files, executable programs and online documents. A major 2020 attack on healthcare companies even hitched a ride on the TrickBot botnet.

5 https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/

The idea of ransomware is so simple it's brilliant: identify a target organization, infiltrate their network, seize control of their assets, then sell back the assets to those who are willing to pay. Instead of a single, large database attack, cybercriminals look to infect as many devices as possible with ransomware and charge victims in return for access to their own files. And ransomware techniques are becoming progressively more brazen; the perpetrators of the Maze ransomware, for example, not only encrypted a victim's data, but also stole it and threatened to release it as a secondary extortion.[6]

Ransomware relies on the fact that the people who will pay the most to retrieve their data are also those who need it the most. Hospitals, for example, cannot take care of patients if their computing resources are inaccessible. Banks can't process payments or conduct financial transactions if they cannot access their networks. Ransomware affects everybody, companies and consumers alike. It is a paralysis that no company can afford.

Neustar International Security Council (NISC) EMEA-US Survey Results[7]

A recent survey of 302 security executives across 7 countries revealed:

54% rank ransomware in their top 3 security concerns.

63% say the threat of ransomware attacks has risen – an increase of **23%** in two years.

6 https://blog.malwarebytes.com/threat-spotlight/2020/05/maze-the-ransomware-that-introduced-an-extra-twist/
7 International Cyber Benchmarks Index, Neustar International Security Council, November 2020

Anatomy of an Attack

Ransomware and data exfiltration attacks initially share the same modus operandi: breach the security barrier through an exploitable weakness. In the case of ransomware, phishing emails are often the vehicle for attack. In fact, statistics from 2020 reveal that more than 97% of all phishing emails contain some form of ransomware.[8]

In these cases, the ransomware is downloaded onto the device or server when the user mistakenly downloads an attachment or clicks a link with vulnerabilities from the phishing email. While users have become experienced in identifying phishing emails—for example, the former finance minister of Zambia probably does not need your help transferring millions of dollars overseas—cybercriminals have also developed more sophisticated attacks that now may be personalized and mimic day-to-day communications such as a jobseeker attaching their resumé to a fake cover letter.

Once the ransomware is downloaded, the attack usually commences quickly. Whereas data exfiltration malware may hide in the network for weeks or months before executing, ransomware attacks are rarely so patient. Instead, they typically execute upon arrival, communicating with an external control server to pass along the encryption key and begin the illegal seizure of data. The encryption process is immediately followed by ransom demands, which usually instruct the victims to deposit payments in an untraceable bitcoin account. If the ransom is not paid quickly, the demands may increase over time (e.g., WannaCry) until action is taken.

Unfortunately, there's no grace period between attacks; victims may be subjected to a second, third, or fourth ransomware attack if they don't address their security vulnerabilities or change their online behavior.

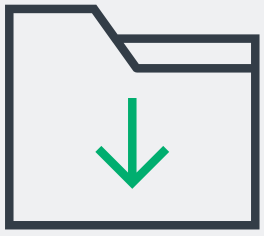
8 https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/

RANSOMWARE STEPS

1

opening phishing email

2



downloading attachment or clicking link

3

communication with external control server

4

encrypt data and generate ransom demand

How to Survive a Ransomware Attack

The truth is, there is no way to prevent being targeted with a ransomware threat. You can, however, prevent it from impacting your business by implementing a multi-layered security approach to thwart future threats.

In our experience at Neustar, we know the best way to mitigate ransomware attacks is to adopt a holistic security strategy that includes:

- A thorough, planned approach to software patch updates and fixes
- Frequent vulnerability and penetration testing from an experienced outside agent
- Update and keep versions of your backup data offline
- Implement phishing prevention and filtering of DNS queries
- Subscribe to threat feeds that can alert you of new and potentially malicious domains
- Be diligent about your security training

How Recursive DNS Can Help

A Recursive DNS server manages outgoing network communications, such as a request to visit a website by providing the appropriate routing information (e.g., IP address) to the external site in question. Recursive DNS servers are also increasingly used for security. For example, when an enterprise network blocks access to a specific site (or types of sites), it's the Recursive DNS server that does the blocking. Because many ransomware attacks rely on communicating with the external control server to initiate the encryption, Recursive DNS servers that incorporate filtering capabilities can prevent DNS-reliant ransomware attacks from occurring by simply blocking the request to activate them.

But not all recursive DNS solutions are equal.

Neustar UltraDNS Firewall is a filtering service built on top of our recursive DNS that blocks the request necessary to activate DNS-reliant ransomware by blocking communication with external command and control (C&C) servers, leaving injected ransomware idle. UltraDNS Firewall also offers additional functionality needed to secure networks against malware and other network attacks, such as:

- Easily creating and implementing security policies that block unauthorized content/access from any device, including remote and mobile devices, using updated third-party threat intelligence.
- Implementing convenient but strong acceptable use policies.
- Eliminating a single point of failure in the event of a DDoS attack, registration flood, or hardware/network issue that could temporarily weaken security.

3 Ways Neustar Helps You Defeat Ransomware

The best way to beat ransomware—or any sophisticated cyberattack—is through a multilayered approach. The security experts at Neustar can effectively help you combat ransomware attacks in three important ways:

1

Professional Security Services

The recency and quick proliferation of ransomware have sent companies scrambling to find experts to assess their vulnerabilities. Our professional services team provides expertise through network vulnerability assessments, resolution of patch/fix issues, disaster recovery planning, and employee training. Neustar can also conduct penetration testing to simulate actual ransomware attacks and demonstrate your network readiness.

2

UltraDNS Firewall

Neustar UltraDNS Firewall blocks access to websites and sources with known vulnerabilities, the simplest way to prevent malware from entering your network. In addition, UltraDNS Firewall cuts off communication with command and control (C&C) servers, rendering many types of ransomware immobile and ineffective. Finally, UltraDNS Firewall makes it easier to identify ransomware, streamlining the removal process, without impacting business operations.

3

DDoS Protection

Cybercriminals are increasingly using DDoS attacks as a smokescreen to mount other attacks, such as ransomware and data exfiltration. Neustar provides advanced DDoS protection to quickly detect and deflect DDoS attacks of all types, including those mounted in conjunction with other attacks.

How We Can Help

To learn more about Neustar Security Solutions, visit us at **www.security.neustar**.

About Neustar.

Neustar is an information services and technology company and a leader in identity resolution providing the data and technology that enables trusted connections between companies and people at the moments that matter most. Neustar offers industry-leading solutions in Marketing, Risk, Communications, and Security that responsibly connect data on people, devices and locations, continuously corroborated through billions of transactions. Neustar serves more than 8,000 clients worldwide, including 60 of the Fortune 100. Learn how your company can benefit from the power of trusted connections.

www.home.neustar

EB-SEC-98529-02.19.2021