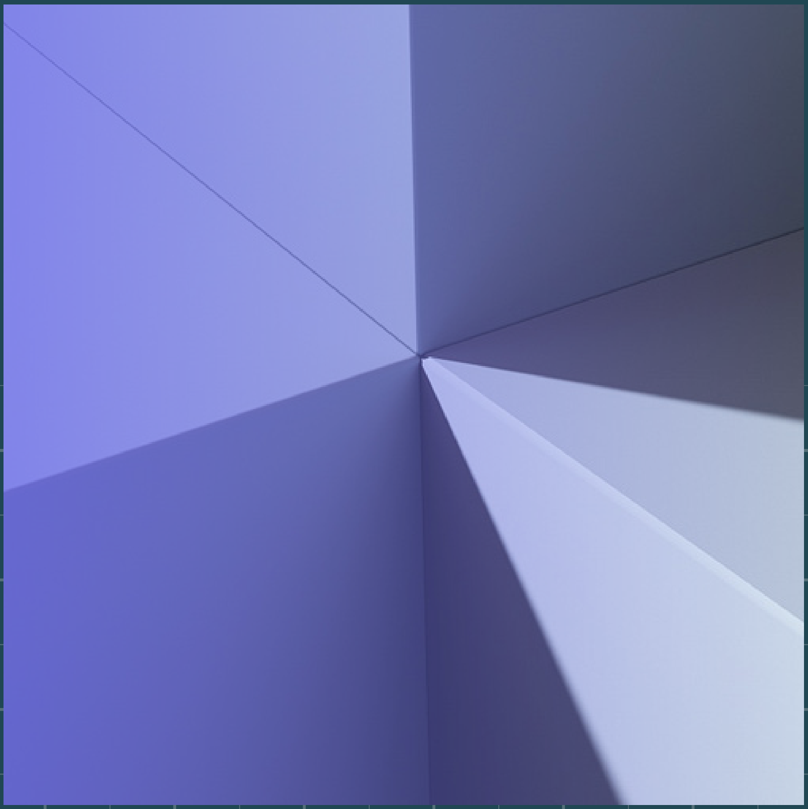
Abnormal

CISO Guide to Ransomware

How It Starts via Email and How to Prevent It

/ By Mike Britton



The Rising Threat of Ransomware

Ransomware, a type of malware that demands a ransom, is becoming an increasing worry for security leaders as it targets more enterprises and causes more damage. When infected with ransomware, organizations lose access to their systems and/or data, often only regaining access after paying hundreds of thousands dollars as part of the ransom.

The debilitating Colonial Pipeline attack in 2021, which cost the organization $4.4 million to restore the data, highlights the devastating consequences of ransomware and why **nearly one in three companies hit with an attack are likely to pay the fee.** Failure to pay the ransom and regain access to important systems can increase the negative customer impact, further damage brand reputation, and present a myriad of other challenges to those attempting to solve the problem.

And when it comes to stopping ransomware before it hits your organization, businesses of all sizes and across all industries must be on alert. Unless we stop these attacks before they reach end users, they will continue to cause severe financial losses and reputational damage—and continue to pad the pockets of cybercriminals.

$200K

The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020.

National Security Institute, 2021

© 2022 Abnormal Security Corporation. All rights reserved.

Types of Ransomware

Despite its popularity, ransomware is not a new threat and has in fact been used by threat actors for more than three decades. The first documented cyber attack using malware dates back to 1989 to a piece of malware targeting AIDS researchers that was delivered via floppy disk.

Now, however, ransomware is used in a variety of more sophisticated ways, including the following.

Cryptocurrency

The biggest driver of ransomware today is cryptocurrency, which became popular around 2013. Because of the relative anonymity of cryptocurrency payments and the low risk of their identity being exposed, cryptocurrency is an attractive option for cybercriminals. Additionally, the ability to send payments via cryptocurrency is frictionless and quick and, perhaps most importantly, the total amount of money that can be sent using cryptocurrency is substantially higher than other payment methods.

As a result, the average amount paid to threat actors in ransomware attacks has skyrocketed from hundreds of dollars just five years ago to tens of thousands of dollars today, with some payments reaching millions of dollars. In fact, travel services company CWT Global set the record for the largest ever ransomware payment via cryptocurrency in July 2020 after paying $4.5 million in bitcoin.

Ransomware-as-a-Service (RaaS)

Like legitimate software-as-a-service companies, cybercrime groups are now able to develop a “ransomware product” and license it to other threat actors in exchange for either a fixed price or a portion of the affiliate’s proceeds. This model is attractive to cybercriminals because it allows technically less sophisticated actors to enter the ransomware space, significantly increasing the number of actors able to carry out an attack.

Extortion

The third type occurs when ransomware actors use extortion tactics, and not just for the initial ransom payment. Until a few years ago, the most common way to prepare for a ransomware attack was to create regular, secure, offline backups of all critical data so in case of a successful attack, any encrypted data could be restored. This changed in 2019 when ransomware actors began exfiltrating those files and threatened to release them to the public if the ransom was not paid. Now, organizations must choose to pay the ransom—or risk having all their files leaked to the public and the shame (and blame) that results from that.

© 2022 Abnormal Security Corporation. All rights reserved.

How Ransomware Works

While ransomware can infiltrate organizations via a variety of methods, there are three common vectors.

Phishing Emails

One of the most common delivery methods is via a phishing email, where the user is encouraged to download an infected attachment or click on a malicious link. When these phishing emails are combined with traditional social engineering tactics, they can entice even the most conscientious user to complete the requested action. And once the user has done so and the malware has been installed, the cybercriminal can take over the victim's computer and use it to complete the rest of their scheme.

Remote Desktop Protocol (RDP) Abuse

RDP is a protocol on Microsoft Windows systems that is designed to allow users to remotely connect to and control a system, such as when IT support needs to control a user's computer to fix an issue. However, RDP is easy to leave exposed on a forgotten system or cloud instance, or alternatively, cybercriminals can use brute force methods to obtain user credentials and thus gain unauthorized access to the RDP system. Once an attacker exploits RDP, they have full access to the system which they can use to lock up systems and then demand their ransom.

Other Security Vulnerabilities

As with other types of threats, ransomware actors are also on the lookout for vulnerabilities they can exploit, and unpatched systems are an attractive gateway to the system. Issues with various web applications, web pages, databases, and web servers can expose server-side vulnerabilities, or web browsers and plugins can expose client-side vulnerabilities, both of which can be used for attack.

Regardless of how the ransomware infects a computer or system, the result is often the same: files will be encrypted and inaccessible without the key known only to the attacker. Of course, that key won't be made available to the victim until the ransom has been paid.

54%

of successful ransomware attacks were delivered via a spam or phishing email.

© 2022 Abnormal Security Corporation. All rights reserved.

Impact of Ransomware Attacks

The FBI's Internet Crime Complaint Center actively tracks losses from ransomware, with 2,474 ransomware attacks reported in 2020. With $29.1 million lost that year, the average attack cost organizations $11,785—far lower than what we've seen with business email compromise and other related cyber attacks.

The caveat here is that this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services used by the victims. These indirect losses can result in a manufacturing plant being shut down or a hospital being forced to transfer patients, or in the case of Colonial Pipeline, it can have repercussions on half of the country as the pipeline ground to a halt. So while ransomware is a relatively low-cost issue at first glance, it's clear that the repercussions are deep.

705%

increase in successful ransomware attacks since 2018.

FBI Internet Crime Complaint Center

$40M

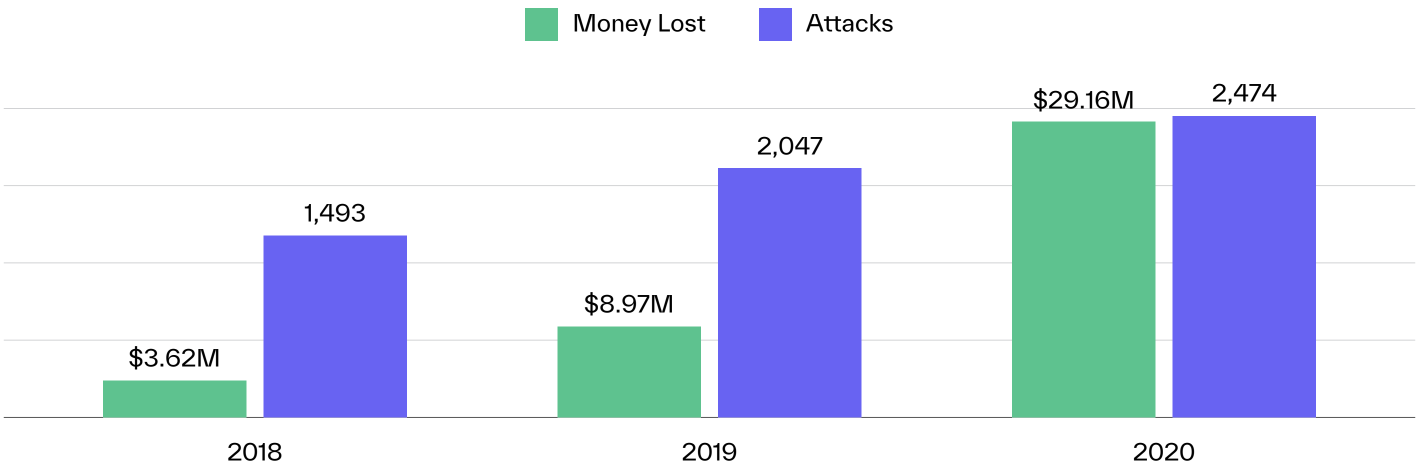
is the largest ransom paid to date.

3.62%

of all advanced email attacks contain malware.

Abnormal Security

Impact of Ransomware Attacks, 2018–2020



FBI Internet Crime Complaint Center

© 2022 Abnormal Security Corporation. All rights reserved.

Why Ransomware Attacks via Email are Successful

While it's clear that ransomware has multiple entry points into an organization, ransomware via email is not likely to dissipate in the near future. In contrast, cybercriminals are only going to get more sophisticated, using social engineering to convince their targets to download the malware. And the traditional email security systems that have protected organizations for years are simply unable to keep up with this new version.

Social Engineering is Evolving

As they see more success with social engineering, we expect threat actors to turn to more sophisticated methods of delivering ransomware via email—concealing it within links in attachments or sending a fake invoice from a known vendor. Alternatively, these threat actors may turn to other file sharing services such as OneDrive or Google Drive, hoping that unsuspecting users will open the attachment without knowing what it contains.

Modern Attacks Outsmart Traditional Defenses

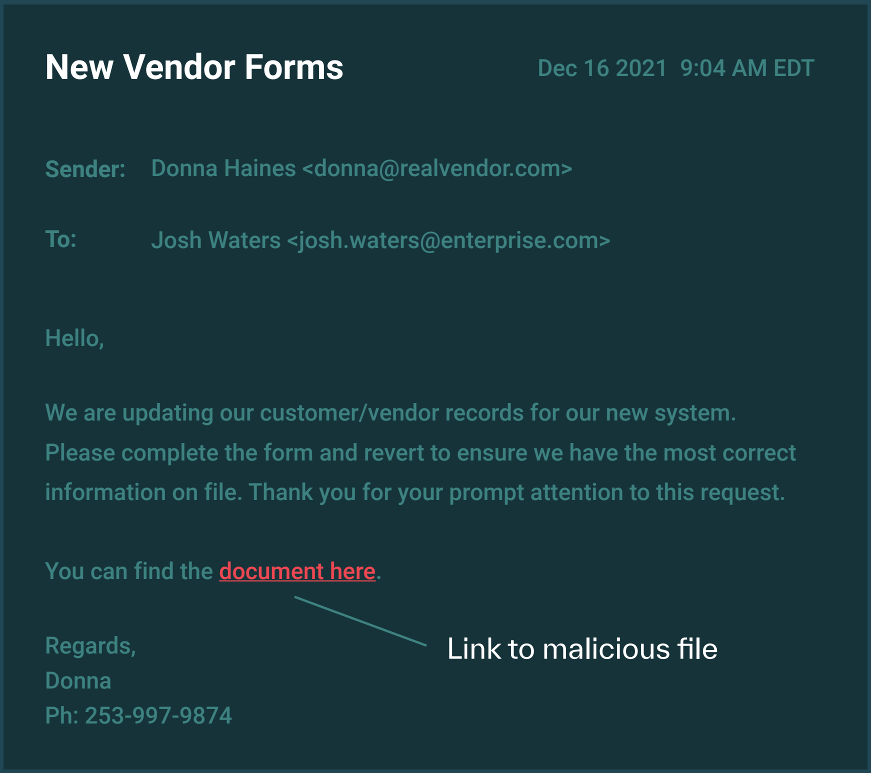
Secure email gateways look for known bad or indicators of compromise, like bad reputation, suspicious links, or malicious attachments. But since ransomware attacks are becoming more sophisticated, these attacks evade conventional defenses, which have known limits on what they can stop.

Security Awareness Training Isn't Enough

For many organizations, security awareness training is used to train employees to spot things like phishing emails so they don't click on malicious links or attachments. However, as threat actors become more sophisticated, it will become even harder to detect what is and is not safe to click. As a result, employees will find it increasingly difficult, if not impossible, to detect when an email contains malware.

© 2022 Abnormal Security Corporation. All rights reserved.

If you look at a real-world example of a ransomware attack that bypassed the secure email gateway, you can see why traditional defenses fail.



New Vendor Forms Dec 16 2021 9:04 AM EDT

Sender: Donna Haines <donna@realvendor.com>

To: Josh Waters <josh.waters@enterprise.com>

Hello,

We are updating our customer/vendor records for our new system. Please complete the form and revert to ensure we have the most correct information on file. Thank you for your prompt attention to this request.

You can find the document here.

Regards,
Donna
Ph: 253-997-9874

Link to malicious file

At first glance, this email does not look malicious. Despite not knowing Donna, the vendor email address is legitimate and it appears that the link itself is safe. However, upon further inspection we can see that this is a Google Docs link that, once clicked, opens a document that provides information on how to download the actual vendor form, which is actually a malicious file. If the recipient were to follow the instructions as Donna has outlined them, they would unknowingly install malware on their computer—all in an effort to ensure that their vendor information is correct.

There is little denying that these attacks are incredibly difficult to detect, by both traditional defenses and humans. As attackers become more cunning, it's increasingly obvious that these emails containing ransomware must be stopped before they can trick your employees.

© 2022 Abnormal Security Corporation. All rights reserved.

How to Stop Ransomware Attacks via Email

To counter these highly-sophisticated social engineering attacks, large enterprise organizations need the right email security platform. The next generation of email security includes:

API Architecture

A solution that connects into Microsoft 365 and Google Workspace via an API, providing access to the signals and data needed to detect suspicious activity. This includes unusual geolocations, dangerous IP addresses, changes in mail filter rules, unusual device logins, and more.

Behavioral Data Science

The solution should use a fundamentally different approach that leverages behavioral data science to profile and baseline goodbehavior and detect anomalies. It should use identity modeling, behavioral and relationship graphs, and deep content analysis to identify and stop emails that include suspicious attachments or links, or unusual download requests.

Automated SOC Operations

The solution should not only detect and block ransomware attempts, but should also make them available for the security team to review. In addition to the information on the sender, the content and tone of the email, and the nature of the request, the SOC team should have access to review the contents of the attachments and the link targets in preview mode. With this information, the security organization can better understand what attacks are entering the organization and better prepare end users to report them.

Without each of these capabilities, ransomware will continue to be delivered through email, outpacing security measures and making it more difficult to prevent these attacks from reaching employees. When they do, they can cause financial losses and lead to data breaches—neither of which a CISO wants to endure.

© 2022 Abnormal Security Corporation. All rights reserved.

Conclusion

There is no doubt that the threat of ransomware is increasing, as losses went from $3.62 million to $29.16 million in just two years. Unfortunately, that number is expected to increase again when the Internet Crime Complaint Center releases the 2021 report—showcasing how cybercriminals are continuing to demand (and receive) their ransoms.

Stopping ransomware delivered via email requires implementing a solution that can detect and interpret thousands of signals through an API, and then block the emails that appear suspicious, even when they do not contain a traditional malicious attachment. It's only by stopping these attacks from reaching inboxes that we can truly ensure that our organizations will stay protected.

/ Mike Britton

CISO, Abnormal Security

Mike Britton is the CISO of Abnormal Security, where he leads information security and privacy programs. Prior to Abnormal, Mike spent six years as the CSO and Chief Privacy Officer for Alliance Data. He brings 25 years of information security, privacy, compliance, and IT experience from a variety of Fortune 500 global companies. He holds an MBA with a concentration in Information Assurance from the University of Dallas.

© 2022 Abnormal Security Corporation. All rights reserved.

Abnormal

Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioral data science to stop socially-engineered and never-seen-before email attacks that evade traditional secure email gateways. Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, ransomware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA.

More information is available at abnormalsecurity.com

Interested in Stopping Ransomware?

Request a Demo:

abnormalsecurity.com →

Follow Us on Twitter:

@abnormalsec

© 2022 Abnormal Security Corporation. All rights reserved.