Information Security Blog › Information Security › How Ransomware's New Breed of "Data Kidnappers" Are Taking Down Global Enterprises and Even Governments

INFORMATION SECURITY NOVEMBER 15, 2018

How Ransomware's New Breed of "Data Kidnappers" Are Taking Down Global Enterprises and Even Governments

JUSTIN DES LAURIERS - TECHNICAL PROJECT MANAGER

SHARE

In part one of this ransomware blog series, we examined how ransomware has evolved over the years. From its beginnings as nuisance pranks and scams mainly affecting home users, today's ransomware "data kidnappers" have evolved, targeting enterprises and governments with dangerous and costly attacks.

In addition to preventing access to critical IT systems, today's advanced and cleverly engineered ransomware can disable public infrastructure such as hospitals and transportation systems—threatening public safety. Let's look at a few recent attacks that have targeted the "bigger fish," ranging from a major shipping port to national golf tournaments to nation states.

Timing is key for many of the data hostage attacks

A particularly disruptive—yet common—type of ransomware attack encrypts enterprise data storage, holding the data hostage until the victim pays the attacker. This was the case in the summer of 2018 when a ransomware attack took down many systems at the Port of San Diego. Part of a growing trend, in return for releasing the data the hackers wanted payment in bitcoin, which—because of the pseudo-anonymous nature of the bitcoin blockchain—is very difficult to trace back to criminals.

Also during the summer of 2018, hackers hit both the Ryder Cup and PGA Championship. After trying to open some marketing files, PGA staff received this threatening message:

"Your network has been penetrated. All files on each host in the network have been encrypted with a strong algorithm. Any attempt to break the encryption could cause the loss of all of the work. This

Subscribe
Email address SUBMIT

TRENDING INFORMATION SECURITY ARTICLES

1 Understanding the Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cybersecurity

2 How Criminals Can Build a "Web Dossier" from Your Browser

3 GDPR and the Security Monitoring Challenge

4 Complying with NY State DFS Regulations with Exabeam

5 Extracting Actionable Information from Windows Events

A key part of the attack was its timing. The ransomware remained dormant until just before the tournament start—at the busiest time for PGA staff—and only then were files encrypted so the ransomware could inflict maximum impact. Highly automated executables with built-in timers and self-contained logic enabled the attack to run autonomously—without requiring detonation orders from a C2 (command and control).

This highlights one way in which this breed of ransomware differs from run-of-the-mill malware—it announces its presence the moment it activates because the hackers want their malicious software to immediately demand payment.

Today's ransomware hackers are "going big"—and causing a lot of damage

Ransomware attacks can have a much larger impact than temporarily denying access to systems in exchange for payment. The demanded ransom amounts often pale in comparison to the collateral damage and downtime costs they cause.

For example, in a massive 2017 attack (which some Western governments maintain the Russian military carried out), NotPetya ransomware targeted companies in Ukraine—hitting government, financial, and energy institutions.

Resultant outages caused extended global damage to entities having a Ukrainian presence, including Maersk, FedEx and Merck. When many of Maersk's—the world's largest container shipping company—80,000 employees around the globe saw their screens go dark, the company lost up to $300 million in revenue, a figure which doesn't include the full-on, emergency rebuilding of its systems infrastructure. Estimates for the total damage caused by NotPetya range as high as $10 billion, making it the most devastating cyberattack in history.

And ransomware hackers aren't stopping with taking down companies—they're now targeting entire nations. For example, the UK's National Cyber Security Centre described WannaCry as a "global coordinated ransomware attack" on thousands of private and public sector organizations across dozens of countries. WannaCry's hard drive-encrypting malware spread very quickly because criminals behind the attack had combined normal malware with a leaked US National Security Agency (NSA) hacking tool. This combination allowed WannaCry to use worm-like capabilities to self-propagate on vulnerable Windows systems. The result was a massive attack that crippled factories, governments, transportation systems and hospitals in more than 150 countries.

Increasingly sophisticated phishing attacks catch even wary users

Phishing email is a ransomware delivery vehicle that has seen a commensurate surge in its prevalence and sophistication. An October 2018 report from the Anti-Phishing Working Group (APWG) says attacks detected in Q2 2018 reached an all-time high—far higher than the same period in 2017.

The number of phishing websites has also grown dramatically—as have those that use encryption (HTTPS). Phishers take the extra step of creating an HTTPS page because they believe the HTTPS URL preface in the browser address field makes their phishing sites seem more legitimate to victims—and thus more successful in catching them. Unfortunately, they're right.

A new breed of phishing bad actors also uses social engineering to dupe sophisticated, high-value targets (e.g., corporate treasurers or other senior staff with access to financial accounts).

1 The Complete Guide to CSIRT Organization: How to Build an Incident Response Team

2 Insider Threats: How to Stop the Most Common and Damaging Security Risk You Face

3 2018 State of the SOC Report

4 5 Best Practices for Your Incident Response Plan

5 How Criminals Can Build a "Web Dossier" from Your Browser

The so-called spear phishers use passwords, personal data, and contacts, as well as other information stolen from sites such as Facebook, or purchased from hackers who have breached entitles such as Verizon, Yahoo! and Equifax. In their virtual confidence games, the spear phishers seek to put recipients at ease so they'll open a file containing a ransomware payload. Or that they'll click on an email-embedded link that takes them to a phishing website where their machine becomes infected.

One spear phishing incident that made the news this past summer is a good example of how such deceptive social engineering works. This extortion ransomware attack laid false claim to having commandeered victims' webcams and microphones, supposedly recording them engaged in uncompromising activities while viewing an adult website. It also showed them a password—current or previous, but one that victim had ostensibly used for the website. The scammer demanded bitcoin in return for not sending the fake, alleged split screen of the respective video recordings to the victims' list of contacts.

But it was the stolen password—offered up by the attacker as evidence of authenticity—that makes this type of extortion (and similar ransomware attacks) so dangerous. The social engineering aspect of using stolen data can fool even sophisticated, tech-savvy consumers or corporate employees.

This proliferation of spear phishing attacks reflects another trend—a shift in targets. In ransomware's ongoing evolution, well-financed developers—representing national military groups to global organized crime rings—are creating ever more complex tools with features that target companies and highly networked environments. Because this is where they can find gold.

What's the window of opportunity to deal with ransomware after infection?

The ideal case would be to detect and stop ransomware before an infection occurs. Unfortunately, this insidious software is almost always detected after the damage has already occurred—it having reached the "payday" stage of the Ransomware Kill Chain (where the hacker demands ransom).

In the first blog of this series, we detailed this kill chain. It begins with a distribution campaign, such as phishing emails, that infect end users' machines and concludes with hackers receiving a ransom payment.

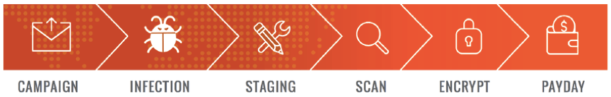
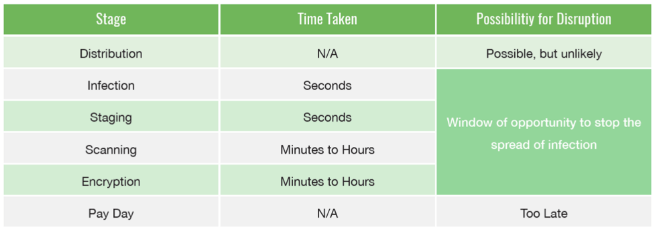


Figure 1 – The ransomware attack chain, from the email campaign to payday

Fortunately, between the kill chain Infection and Encryption phases you have an opportunity to disrupt the process. During these phases, ransomware needs to install itself, prepare to persist past rebooting, identify vulnerable files, then encrypt those files. Each phase takes time, although in some cases not a lot of it. Depending on the type of environment a given victim has, scanning and encryption can take anywhere from minutes to hours.

For personal computers, files are typically relatively low in number and stored in very easy to find locations, such as local or external hard disks, or even cloud storage such as Dropbox. For these relatively simple environments, the malware may complete scanning and encryption in minutes. This leaves a relatively shortened duration to detect and react to an incident.



Stage	Time Taken	Possibilitiy for Disruption
Distribution	N/A	Possible, but unlikely
Infection	Seconds	Window of opportunity to stop the spread of infection
Staging	Seconds	
Scanning	Minutes to Hours	
Encryption	Minutes to Hours	
Pay Day	N/A	Too Late

Figure 2 – Potential detection duration during each Ransomware Kill Chain phase

In corporate networks, ransomware has a much larger job to do in identifying assets, file shares, network drives, cloud drives, and other machines to infect. Network mapping, file identification, and permission checking could take hours. And the bigger the network, the longer this process will take.

The same is true for encryption. A greater number of vulnerable files means more encryption must happen before victims can be presented with a ransom demand.

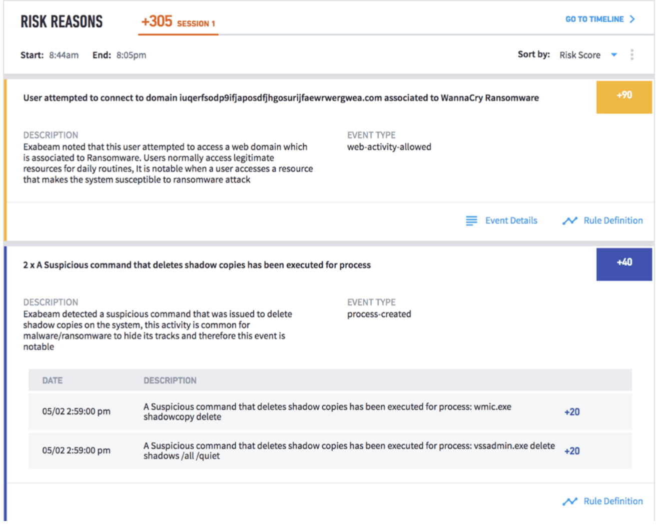
For your security analysts, it's critical to detect and interrupt the ransomware kill chain during the available opportunity window. By doing so they can stop the spread of the infection and quarantine affected machines, removing them from the network until they can be treated.

A behavioral approach can help you interrupt the Ransomware Kill Chain

One way to thwart a ransomware infection—before it begins to encrypt your files—is by deploying user entity behavior analytics (UEBA), which can detect the telltale behaviors associated with ransomware. It lets you identify an attack earlier in its kill chain, such as during the Infection, Staging, or Scanning phases, before encryption occurs.

Using models and rules to track user behavior—a behavior-based approach offers an ideal way to detect ransomware attacks. From the onset of its deployment, a behavior-based approach creates normal user behavior baselines, making it possible to track any deviations from the norm. Examples include an illegitimate user who attempts to connect to a domain, or an insider who suspiciously downloads files typically not associated with them.

With Exabeam's UEBA, rules also detect the first-time appearance of files and processes. Such risky behavior could be an indicator of malicious activity and is bubbled up, such as the example in Figure 3.



Start: 8:44am End: 8:05pm

User attempted to connect to domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com associated to WannaCry Ransomware +90

DESCRIPTION
Exabeam noted that this user attempted to access a web domain which is associated to Ransomware. Users normally access legitimate resources for daily routines, It is notable when a user accesses a resource that makes the system susceptible to ransomware attack

EVENT TYPE
web-activity-allowed

2 x A Suspicious command that deletes shadow copies has been executed for process +40

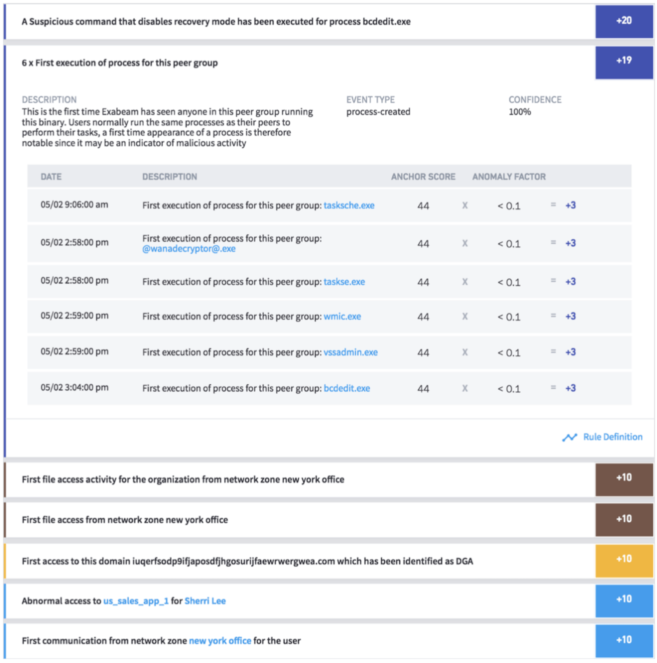
DESCRIPTION
Exabeam detected a suspicious command that was issued to delete shadow copies on the system, this activity is common for malware/ransomware to hide its tracks and therefore this event is notable

EVENT TYPE
process-created

DATE	DESCRIPTION	
05/02 2:59:00 pm	A Suspicious command that deletes shadow copies has been executed for process: wmic.exe shadowcopy delete	+20
05/02 2:59:00 pm	A Suspicious command that deletes shadow copies has been executed for process: vssadmin.exe delete shadows /all /quiet	+20

Figure 3 – UEBA model rules detecting a user attempting to connect to a malicious domain

Exabeam behavior analytics track any first-time binary execution on peer groups, first-time file access by remote groups, abnormal access to cloud services, first-time file access from remote locations, and more. And it provides rules to detect any abnormal network file activities.



A Suspicious command that disables recovery mode has been executed for process bcdedit.exe +20

6 x First execution of process for this peer group +19

DESCRIPTION
This is the first time Exabeam has seen anyone in this peer group running this binary. Users normally run the same processes as their peers to perform their tasks, a first time appearance of a process is therefore notable since it may be an indicator of malicious activity

EVENT TYPE
process-created

CONFIDENCE
100%

DATE	DESCRIPTION	ANCHOR SCORE		ANOMALY FACTOR		
05/02 9:06:00 am	First execution of process for this peer group: taskche.exe	44	X	< 0.1	=	+3
05/02 2:58:00 pm	First execution of process for this peer group: @wanadecryptor@.exe	44	X	< 0.1	=	+3
05/02 2:58:00 pm	First execution of process for this peer group: taskse.exe	44	X	< 0.1	=	+3
05/02 2:59:00 pm	First execution of process for this peer group: wmic.exe	44	X	< 0.1	=	+3
05/02 2:59:00 pm	First execution of process for this peer group: vssadmin.exe	44	X	< 0.1	=	+3
05/02 3:04:00 pm	First execution of process for this peer group: bcdedit.exe	44	X	< 0.1	=	+3

Rule Definition

First file access activity for the organization from network zone new york office +10

First file access from network zone new york office +10

First access to this domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com which has been identified as DGA +10

Abnormal access to us_sales_app_1 for Sherri Lee +10

First communication from network zone new york office for the user +10

Figure 4 – Exabeam detecting abnormal remote access and first-time access to a malicious domain

In addition to creating timelines that show all relevant events, using UEBA lets investigators automate responses and block and contain malware, thereby preventing it from spreading.

For more information on the anatomy of ransomware attacks and how UEBA can help you mitigate them, see the Exabeam Ransomware Threat Report.

#RANSOMWARE

JUSTIN DES LAURIERS
TECHNICAL PROJECT MANAGER

More like this

If you'd like to see more content like this, visit the Exabeam Blog

Explore more

INFORMATION SECURITY

Operation Aurora – 2010's Major Breach by Chinese

INFORMATION SECURITY

Exabeam's Top Cybersecurity Blog Posts of

UEBA

User Behavior Analytics (UBA/UEBA): The Key to

Hackers

JANUARY 8, 2019 — TIM MATTHEWS

Exabeam's Cybersecurity History Review: Read about Operation Aurora and the series of cyberattacks in 2010 conducted by the Elderwood Group based in Beijing, China, with ties to the People's Liberation Army.

2018

JANUARY 2, 2019 — MARITZA MARIE DUBEC

2018 was a memorable year for cybersecurity. Millions of people were impacted as we saw more companies hit by megabreaches—from a major hotel chain to a social media platform used by billions. Here are our top 10 blog posts that had the biggest readership and were the most noteworthy.

Uncovering Insider and Unknown Security Threats

JANUARY 2, 2019 — ORION CASSETTO

Learn about UBA technology, and its extension UEBA (User Entity Behavior Analytics), how it works, and which threats it uncovers that no other tool can see.

Exabeam provides security intelligence and management solutions to help organizations of any size protect their most valuable information.

REQUEST A DEMO

PRODUCT
- Exabeam Advanced Analytics
- Exabeam Cloud Connectors
- Exabeam Data Lake
- Exabeam Entity Analytics
- Exabeam Incident Responder
- Exabeam Spectrum
- Exabeam Threat Hunter

ANALYST CORNER

PARTNERS

SUPPORT

SOLUTIONS
- Compliance
- Threat Detection
- Cloud Security
- IoT Monitoring
- SOC Automation

ABOUT

CAREERS

MEDIA KIT

LEARN
- Library
- Newsroom
- Glossary
- SIEM Cost Comparison

BLOG
- Information Security
- SIEM
- UEBA
- Security Operations Center
- DLP
- Incident Response

SIEM GUIDE
- What is SIEM?
- SIEM Architecture
- Events and Logs
- UEBA
- SIEM Use Cases
- SIEM Analytics
- The SOC, SecOps and SIEM
- Incident Response and Automation
- SIEM Buyer's Guide

CONTACT

2 Waters Park Dr., Suite 200
San Mateo, CA 94403

1.844.EXABEAM

info@exabeam.com

Terms & Privacy Policy — Sitemap