exabeam

THREAT RESEARCH REPORT
THE ANATOMY OF A RANSOMWARE ATTACK

INTRODUCTION

Most malware is silent or at least seemingly so. It hides itself deep inside infected machines to stealthily carry out its mission. Communication to the outside world, in order to receive commands or send stolen data, is usually hidden. The reason for this discrete behavior is simple, to avoid detection by users and their security controls, thus buying time to steal credentials, exfiltrate data, or compromise additional systems. This is not the case with ransomware.

One of the most glaring differences between typical malware and ransomware is that the second ransomware finishes its activity; it announces its presence to the user. It does this because it has already taken the victim's machine and files hostage and wants to demand ransom in exchange for the return of these assets. Ransomware is also highly automated, such that beyond the "distribution stage", most of the ransomware process runs autonomously without requiring communication with a C2 (command and control) to receive instructions. Instead ransomware executables contain all the logic required to hijack a computer.

To further compound the problem, ransomware has only recently begun targeting corporations, which means that most security analysts have not yet had the opportunity to observe how ransomware behaves within corporate environments. This makes it difficult for analysts to detect ransomware early enough in the ransomware lifecycle to stop it.

This confluence of factors sparked our interest in researching ransomware behavior. By exposing our findings to the security community we hope security analysts everywhere will better understand this type of malware. Armed with this information, analysts should be able to react faster in the event their organization is hit with a ransomware infection.

DEFINING THE RANSOMWARE KILL CHAIN

After detonating 86 strains of ransomware in our lab, we were able to narrow down the phases of the ransomware's activity to six stages that assemble the "Ransomware Kill Chain". These six stages were ubiquitous across all the strains we tested, and consistent in the face of permutations or improvements to any specific strain.

The main stages of the Ransomware Kill Chain are as follows:

1. **Distribution campaign** – attackers use techniques like social engineering and weaponized websites to trick or force users to download a dropper which kicks off the infection
2. **Malicious code infection** – the dropper downloads an executable which installs the ransomware itself
3. **Malicious payload staging** – the ransomware sets up, embeds itself in a system, and establishes persistency to exist beyond a reboot
4. **Scanning** – the ransomware searches for content to encrypt, both on the local computer and the network accessible resources
5. **Encryption** – the discovered files are encrypted
6. **Payday** – a ransom note is generated, shown to the victim, and the hacker waits to collect on the ransom

A DETAILED LOOK INTO THE RANSOMWARE BUSINESS

Similar to more traditional (and legitimate) businesses, ransomware operators are constantly evolving their networks and looking to optimize their businesses. The assembly of a ransomware operation is largely made up of three distinct tasks: software creation and hosting, distribution, and ransom collection. Based on who has responsibility for each of these steps, we noticed three common operational models which are employed by the vast majority of ransom networks. Interestingly, these models bear strong resemblance to those used in the B2B software world.

With clearly defined business models, a wide array of targets, and different roles and payouts that match various levels of technical prowess; joining a ransomware operation is an attractive option for would-be cyber criminals. In the following section, this paper will explore the three most prevalent operations models for ransomware networks.

MODEL 1: VERTICALLY INTEGRATED BUSINESS

Vertical integration, or the control of a supply chain from end-to-end by a single company, is nothing new in technology. With companies like Apple proving how profitable it can be to own operations in their entirety, it's no surprise that many ransomware networks have also selected this as a common business method. In this model, the hacker or group of hackers is responsible for their entire ransomware operation. They are the ransomware software developer, responsible for hosting that ransomware and its associated droppers, they must manage its distribution methods (spam, weaponized websites, etc.), and also collect the ransom.

By using this model, hacking groups are able to retain 100% of the profits from their ransomware. However, managing all aspects of operation creates a high entry barrier for hacking groups, since the group will need talented people to perform each aspect of the campaign. The image below provides an example of what a vertically integrated ransomware operation might look like.

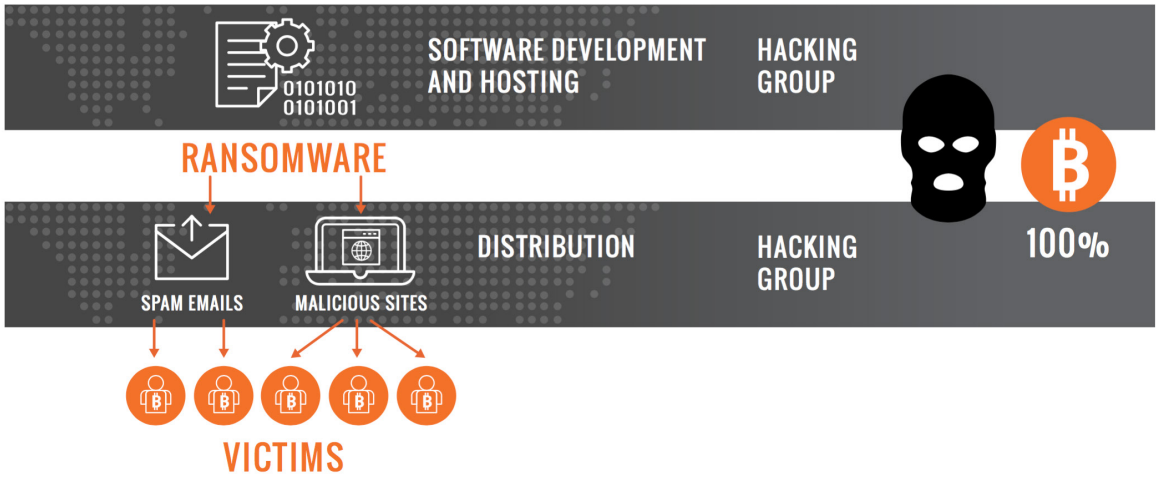

Figure 2. An illustration of the responsibilities and margins for a vertically integrated model

MODEL 2: ESTABLISHING A RESELLING CHANNEL WITH AFFILIATE GROUPS

While crucial for achieving scale, the task of ransomware distribution is particularly effortful. Successful distribution hinges on the creation and execution of well-crafted spam campaigns, or weaponizing popular websites with drive-by-downloads that infect victim machines. These tasks come with a higher risk of detection and require vastly more effort than developing the ransomware itself. For this reason, it's common for hacking groups to outsource the distribution of their ransomware to groups that specialize in distribution.

These distribution groups function very similarly to the distribution channels used to sell enterprise software. Interested parties apply through an affiliation program that pays pre-determined margins on completed ransoms that are a result of that affiliate's distribution efforts. Payouts for distribution groups usually range between 50% to 75% of the ransom obtained from the victim.

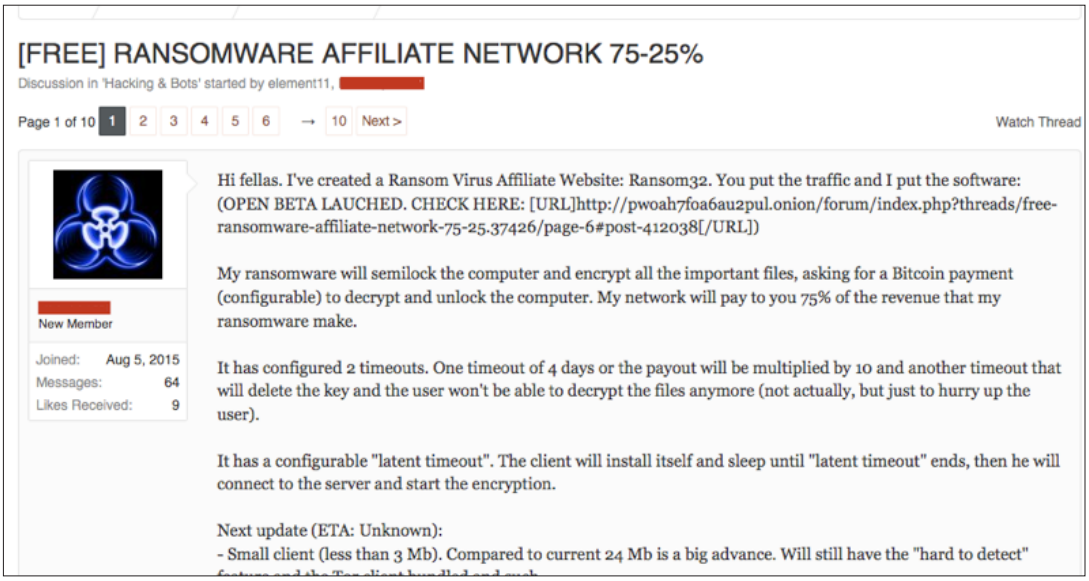

Figure 3. Ransomware affiliation network offering on a dark web marketplace

With an affiliate relationship in place, the software is still developed and hosted by the hacking group, and the ransom is collected by the hacking group, but distribution is completely handled by the distribution group. The image below illustrates provides an example of how a distribution model works.

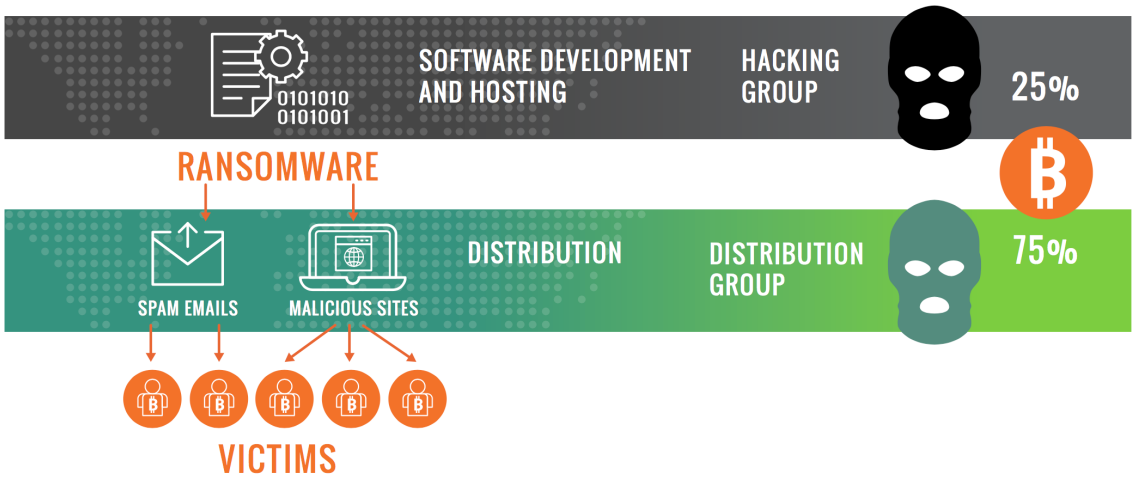

Figure 4. An illustration of the responsibilities and margins for an affiliation network

Many ransomware networks go so far as to require the payment of "affiliate onboarding fees" for new affiliates that wish to join their network. These one-time membership fees typically range from $500-$1500-USD. The turn-key nature of these affiliate programs has earned this model the moniker RaaS (Ransomware as a Service).

MODEL 3: RANSOMWARE "MANAGED SERVICE PROVIDERS"

The third and final model that we observed is most analogous to the Managed Service Provider model of the enterprise software world, where service providers purchase products from vendors and turn them into services that they sell to their customer base. In this model, a distribution group purchases ransomware software directly from the hacking group for a license fee that ranges between $1K and $100K USD.

Once a distribution group has purchased the required software, it is responsible for all aspects of the ransomware operation including hosting, distribution, and ransom collection. By leveraging this model, they earn 100% of the ransom they collect.

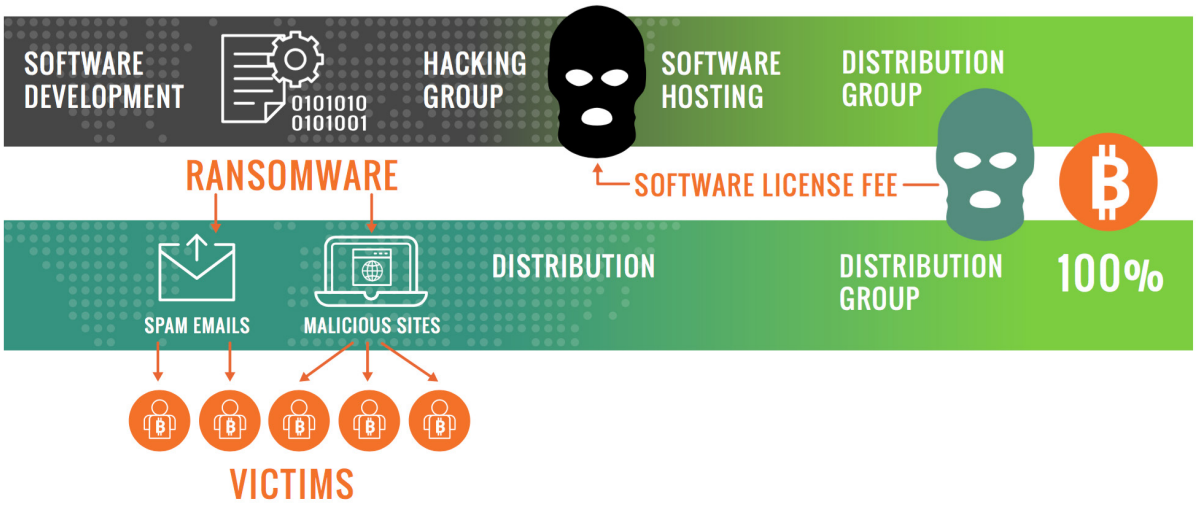

Figure 5. An illustration of the responsibilities and margins for distribution groups who purchase ransomware software from a hacking group

THE BUSINESS OF RANSOMWARE: PRICING AND THE PAYDAY

A recent trend in the ransomware landscape that we observed during the course of our research was a rise in the price of ransoms. A few months ago, the average ransom for an infected machine was around 0.5-1.25 Bitcoins (BTC) which was the equivalent of roughly $300-$800 USD at the time of writing. However, with ransomware's success, the prices of ransom seem to be climbing. For example, we noticed that the ransom demanded by Cerber, a popular ransomware, climbed from an average of 1.25 BTC to 2 BTC; and Locky went from 0.5 BTC to 5 BTC (~$2,800 USD) during the same timeframe. It is important to point out that ransom amounts fluctuate from campaign to campaign, and from strain to strain.

The impetus for price increase may also have its roots in another fundamental change in the ransomware landscape, a shift in targets. Increasingly, ransomware developers are creating more complex tools with features that are designed to target companies and highly networked environments rather than individuals. These features include network scanning and shared-drive encryption. With companies as targets, the data being held hostage tends to be more valuable, and the fact that companies usually have deeper pockets than individuals, means they are more likely to pay ransoms even if they come with a higher price-tag.

Figure 6. Locky ransomware ransom payment page, priced at 5.00 BTC as of May 27, 2016

Another important aspect to ransomware pricing is the timeliness of payment. A common feature of many ransomware strains is the ability to become more aggressive if payment terms are not met within the pre-determined payment period. For many ransomware specimens this results in a large multiplier being applied to the ransom. We've seen anything from a 2x to 10x multiple being added to ransom demands for tardiness.

DISSECTING THE KILL CHAIN: ACTIVITY AND ARTIFACTS

After careful analysis of all 86 ransomware specimens, we found a surprising amount of commonality in their behavior. Ultimately, because these strains share a common goal of demanding ransom, the activities they must perform to reach this goal are the same. We assembled the following Ransomware Kill Chain from the six stages which are shared by all ransomware strains:

DISTRIBUTION CAMPAIGN

The first stage in the kill chain is distribution of the installation software to potential victims. During the distribution campaign, users are tricked or forced into downloading and activating a malicious dropper or payload via an email, a watering-hole attack, an exploit kit, or a drive-by-download. This dropper is responsible for kicking off the infection.

INFECTION

Once on the victim's machine, the dropper phones home to download an .exe or other camouflaged executable by connecting to a predefined list of IP addresses that host the C2 server, or by using DGA to connect via pseudo random domains. From this point, the dropper usually copies the malicious executable to a local directory such as Temp folder or %AppData%/local/temp. Finally, the dropper script is terminated, removed, and the malicious payload is executed.

STAGING

During the Staging phase, the ransomware performs various housekeeping items to ensure smooth operation, such as moving itself to a new folder then dissolving, checking the local configuration and registry keys for various rights, such as proxy settings, user privileges, accessibility, and other potentially meaningful information.

The ransomware also performs several persistence steps into the system, such as running at boot, run when in recovery mode, disabling recovery mode, etc. Finally, it uses various commands to delete shadow copies of the files from the system. Ransomware also communicates with C2 at this stage to either get the ransomware's public key negotiated, or to perform recon on the user/system using online IP analytic tools to determine whether or not they are an applicable target.

SCANNING

Now that the ransomware has set itself up, and is equipped to persist in the face of shutdowns or reboots, it prepares to take files hostage. To do this, the Ransomware enumerates both the local system and network-accessible systems, searching for a predefined list of file extensions of interest. The ransomware scans and maps the locations containing those files, both locally and on both mapped and unmapped network-accessible systems. Many ransomware variants also look for cloud file storage repositories such as Box, Dropbox, and others; which may also be included.

The scanning phase presents security analysts with the first real opportunity to interrupt the Ransomware Kill Chain. While scanning the local machine and synced cloud folders can be accomplished in seconds, mapping out a large corporate network, investigating the results of the scan, checking for read and write permissions, etc. can take minutes to hours depending on the amount of information which must be assessed.

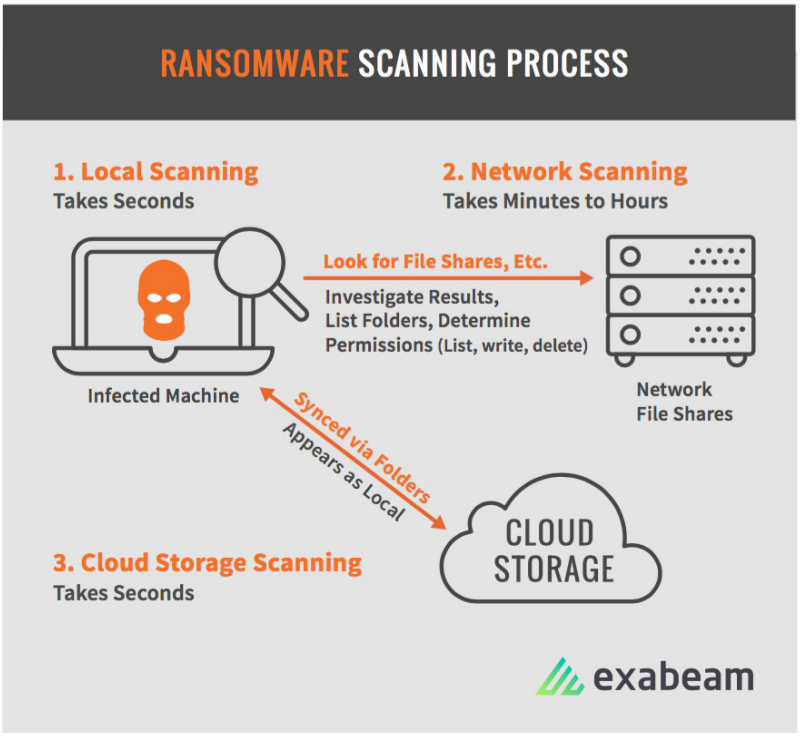

Figure 7. The Ransomware Scanning Process

ENCRYPTION

Until the encryption phase, nothing potentially irreversible has happened. The ransomware has simply unpacked itself and performed reconnaissance on the system within which it exists. Beginning with the Encryption phase, control of the situation begins to tilt in favor of the hacker as the ransomware begins to encrypt all of the files it discovered while scanning. Much like the scanning phase, the encryption phase can take minutes to hours.

All encryption happens locally on the infected machine, meaning that for each file that must be encrypted, the ransomware must fetch the file, encrypt it, upload the newly encrypted version to the original location, and then delete the original file.

For every location where files have been found and encrypted, copies of auto-generated ransom notes are created in multiple formats, including .html, .txt, and scripts. With ransomware we see an interesting correlation between company size and ability to respond; the larger an organization is, the more likely security analysts or DFIR teams will be able to stop an infection before this process is complete. This is due to the amount of scanning and encryption which must take place before ransom can be demanded.

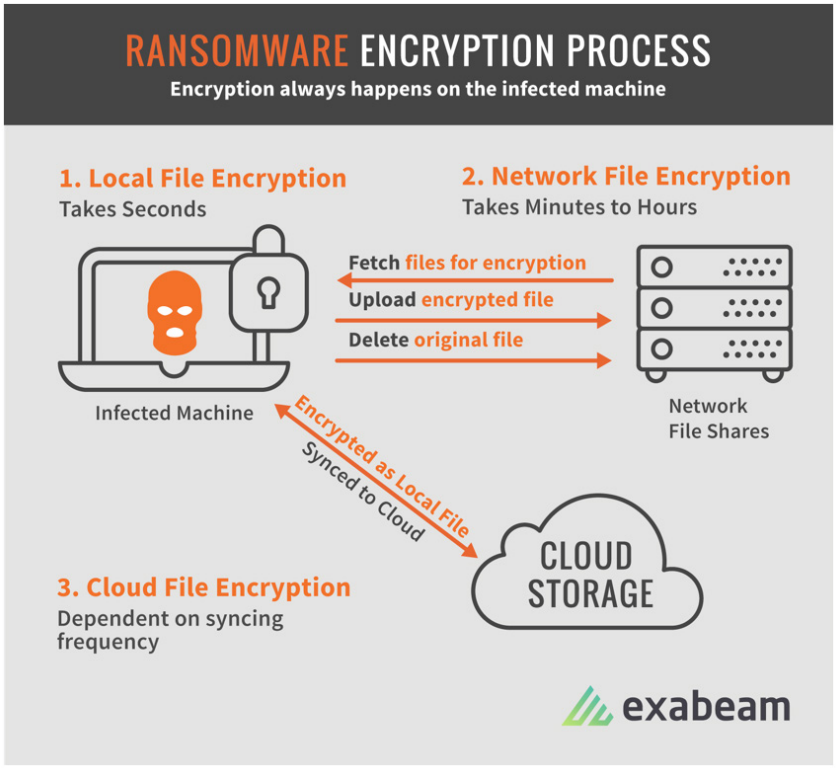

Figure 8. The Ransomware Encryption Process

Should network storage or cloud storage locations that were discovered during the scanning phase become unavailable, the ransomware can lay dormant (relying on its persistency precautions taken during staging) and wait patiently for them to become available for encryption again.

PAYDAY

Once encryption is complete, the ransomware explicitly displays a ransom note to the victim. A common way to do this is to change the desktop wall paper to a ransom note that includes payment instructions. With its mission complete, the last task the ransomware usually performs is to terminates and delete itself.

At this point, hackers simply wait for ransom to be paid to a bitcoin wallet they own. Victims on the other hand must decide whether to pay the ransom or part ways with the files which were encrypted by the ransomware. As noted during the payment section of this paper, many types of ransomware are pre-configured to have timeout thresholds where the ransom price increases or the software begins to delete encrypted files. After ransom has been paid, victims are typically provided with a link they can use to download a key or decryption program.

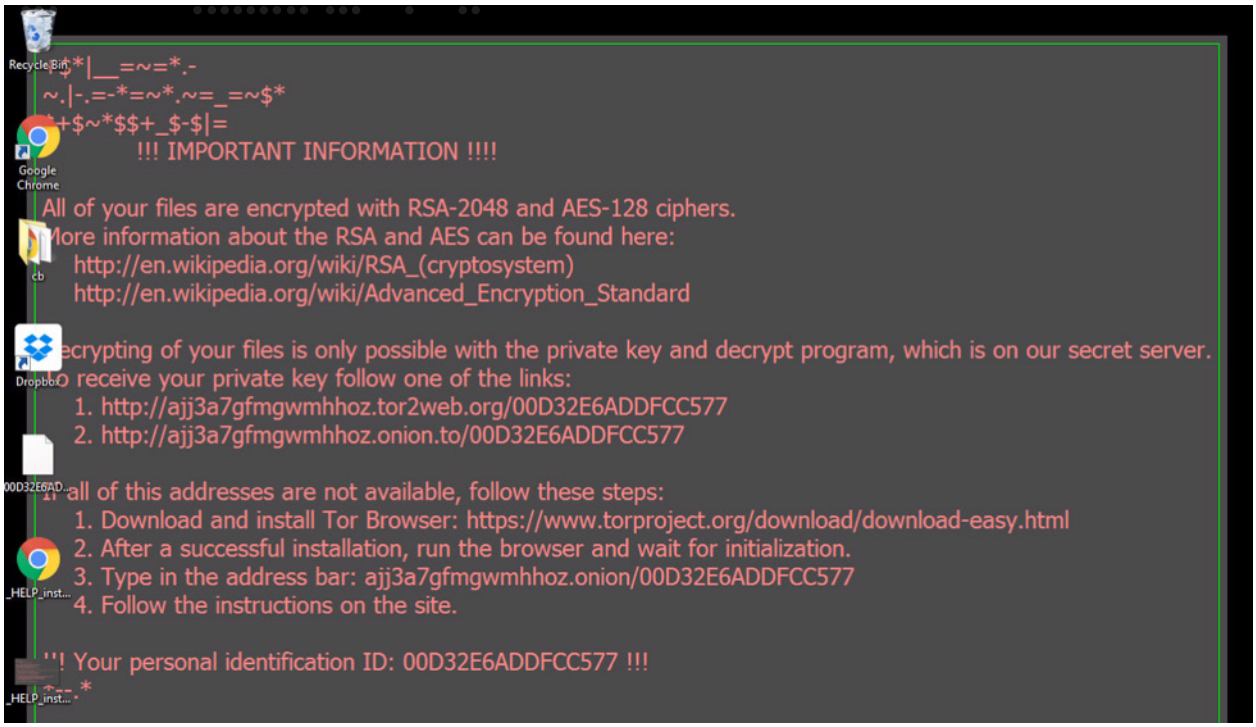

Figure 9. An example of a ransom note posted to the desktop wallpaper of an infected machine during the payday phase

DEALING WITH RANSOMWARE

Ultimately, in many organizations the task of cleaning up ransomware falls squarely on the shoulders of the security analysts within an organization's Security Operations Center. For these analysts, experience is the difference between quickly addressing a problem and a lengthy investigation. If the analyst on duty has dealt with an issue before, addressing the problem will be much smoother than if they have to piece it together from scratch. Unfortunately, virtually no security analysts or DFIR teams have had the opportunity to deal with ransomware at the scale necessary to holistically understand the problem. If an analyst does understand ransomware enough to identify it as it's happening, they still need to piece together a timeline of the incident in order to understand the scope and impact of the infection, for example which systems and assets were affected. This eats up valuable time which could otherwise be used to stop the infection.

After countless hours in the lab detonating various strains of malware and recording the affects, we've put together the following recommendations on how to handle a ransomware infection.

PREVENTION

The age old adage "an ounce of prevention is worth a pound of cure" certainly holds true for ransomware. Stopping ransomware before it gets a foothold in an organization would be ideal. This is possible to do at the tail end of the campaign stage, where distribution is happening via an email or drive by download.

There are vendors working hard at finding ways to reduce the viability of ransomware distribution campaigns by defending websites from infection to prevent watering hole and drive-by-download attacks, by preventing spam messaging from reaching recipients, and by scanning executables for signs of ransomware. These are welcome efforts however, infection is still a very real risk. Additionally, if we've learned anything from the anti-virus industry, it is that there is no silver bullet for security. Attackers will evolve their distribution methods and find ever-inventive ways to infect their victims.

TIME TO DETECTION MATTERS... A LOT

While we wish that all ransomware could be stopped prior to infection, this is simply not realistic in most cases. Ransomware is almost always detected after the damage has already occurred and the software has already reached the "payday" stage, where ransom is being demanded.

Fortunately, between the Infection and Encryption phases in the kill chain there is an opportunity to disrupt the process. During these phases, ransomware needs to install itself, prepare to persist past rebooting, identify vulnerable files, and finally encrypt those files. All of these things take time, albeit in some cases not a lot of it. Depending on the type of environment a victim has, scanning and encryption may 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 file storage service like Dropbox. For these relatively simple environments, scanning and encryption may be completed in minutes. This leaves a relatively short period of time to detect and react to an incident.

In corporate networks, ransomware has a much larger job to do in terms of identifying assets, file shares, network drives, cloud drives, other machines to infect, etc. 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. More vulnerable files mean more encryption must happen before victims can be presented with a ransom note demanding payment. This provides a window of opportunity illustrated below.

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 10. An illustration showing the amount of time that potentially exists during each phase of the kill-chain

For security analysts, it's critical to detect and interrupt the ransomware kill chain during their window of opportunity. 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.

DETECTING RANSOMWARE – WHAT WORKS?

During our lab analysis, we noticed a consistent trend amongst the various specimens we dissected, frequent change. Each software updated itself daily, such that we didn't observe a single piece of ransomware that remained unchanged for longer than a 24-hour period. This provides ransomware networks the benefit of remaining one step ahead of the AV vendors, signature-based security solutions, and threat intelligence solutions since any signatures, domains, or IP addresses associated with the ransomware would be obsolete within a 24-hour period.

When signatures are absent or ineffective, detection must rely on other approaches. We found that ransomware can be reliably detected using behavioral modeling. Based on the goal of reaching the Payday, or ransom stage of an infection, these programs logically must first distribute themselves, infect a system, stage their environment, scan for data to encrypt, encrypt it, and then finally inform the users what it has done.

Ransomware by definition has the specific goal of holding files hostage in exchange for payment. This predictable goal yielded us an easily definable kill chain or lifecycle which can be tracked using behavioral analysis. Each stage in the kill chain has specific activities that must happen to complete that stage and those activities will manifest themselves in log artifacts as actions the infected user has taken.

These log artifacts are things like file activity logs, registry tracking logs, endpoint security system alerts, etc. By analyzing all log artifacts from a specific environment, both good and bad, and tying them back to specific users, the timelines of each users' daily activity can be created. Behavioral modeling can then determine what is normal and abnormal behavior for these users and identify anomalies associated with ransomware in real-time.

It is essential that this behavioral modeling makes use of automated techniques in order to accomplish this analysis within the window of opportunity in the ransomware kill chain. Relying on human-based analysis to piece together the signs of a ransomware infection would be error prone, and time consuming such that detection before the pay-day stage would be highly unlikely.

WHAT ELSE CAN BE DONE ABOUT RANSOMWARE?

Aside from the real-time ransomware detection described above, there are several steps that security teams can take in order to better equip themselves to deal with the threat of ransomware.

- **Back up Files** – frequent backups of critical files will allow documents to be recovered even if ransom is not paid.
- **Security Training** – Occasional training sessions can help educate employees on how to avoid becoming the victim of spam attacks or weaponized websites.
- **Security Analyst Education** – Provide security analysts and digital forensic and incident response (DFIR) teams with opportunities to learn about threats. This will help them identify and react to security incidents in their environment.

SUMMARY

Ransomware, while unique from other malware, still exhibits several tell-tale signs which can point out an infection underway. By analyzing users' day-to-day behavior in real-time for the anomalies we've discussed in this paper, it may be possible to detect these early warning signs and stop a ransomware infection dead in its tracks. To help better identify these activities and what log artifacts house them, we've included a Security Analyst Ransomware Cheat Sheet to the final page of this document.

For more information, please visit http://www.exabeam.com, or send email to info@exabeam.com.

GLOSSARY OF TERMS

C2 – an abbreviation that stands for "command and control". C2s are servers or networks used by machines infected with malicious code to receive commands and stolen data. C2 servers can be distributed in layers to prolong their activity and hide the origin of commands.

DFIR – An acronym that stands for Digital Forensics and Incident Response. The DFIR team is in charge of discovering, handling, and mitigating security threats.

Drive-by-download – A download in which a person is unknowingly tricked into downloading malicious code with a download that either appears legitimate, or is masked as part of a bigger flow of activity. A weaponized website is a common way for drive-by-downloads to infect victims.

Water-hole attack – A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.

Exploit kit – a software kit designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it, and discovering and exploiting vulnerabilities to upload and execute malicious code on the client. (source: Wikipedia)

Dropper – a piece of code designed to download and install the actual malware payload in an obfuscated way which evades detection. Since the dropper is usually a small and simple program, it is often short lived and frequently mutates while the malicious malware payload may stay the same. The Dropper may also include initial commands to the Malware such as DGA seed or IP addresses with which to communicate.

DGA – Domain Generating Algorithm, sometimes referred to as AGD (algorithmically generated domain) is a technique where Malware can generate domain names based on predefined technique such as a seed or number which is also known to the C2 and is dynamically registered by it. DGA therefor allows the malware and backend to establish a connection without a predefined domain name

SECURITY ANALYST RANSOMWARE CHEAT SHEET

Kill Chain Stage	Examples of Observed Ransomware Activites	Log Artifacts
Distribution	• Either an email or a web activity log showing the incoming file via either a download or an email attachment. In the most common test case, we noticed that an email with an attachment coming from a domain that had never sent an email to anyone in the company	An email Proxy Firewall IPS
Infection	• A new process on a computer is observed in process logs where the dropper is activated and read as a new process, from a new location • The process communicates to the world with a domain that can be usually identified as DGA (domain generation algorithm) artifact • A file that has been downloaded is then either renamed or ran from an unusual place such as a temp directory or a cache directory and is a new process for the user or the machine. • A process that runs another process and then dissolves is observed	Proxy File activity Process tracking
Staging	• A process that has not been seen in the enterprise before creates a randomly-named executable or an executable with the name of a Windows component but in the wrong path • A process adds an entry to an autorun location, such as the Startup folder or the Run key in the Registry • A process launches a command prompt and deletes shadow copies or modifies boot options • A newly-created process uploads data to a newly-registered domain or to a bare IP	File activity Process tracking Registry tracking Proxy Endpoint security
Scanning	• A set of authentication logs showing scanning-type activity coming from the compromised host • A process in a temporary location, or a process with a known-name but in a new location, enumerates a large number of local directories	Authentication File activity Network activity Process tracking
Encryption	• A process reads, creates, and deletes files from an unusual number of directories • Files are created with known-bad, suspicious, or unusual extensions • A process reads, creates, or deletes files in directories it doesn't normally access • A process creates many copies of a small set of files in a large number of directories	Authentication File activity Process tracking logs
Payday	• A process running from an unusual place spawns a web browser and/or Notepad with command line arguments • The desktop background is changed	File activity Process tracking

For more information, please visit http://www.exabeam.com, or send email to info@exabeam.com.