White Paper

Security

Best Practices for Ransomware Mitigation, Detection, and Response

MICRO FOCUS

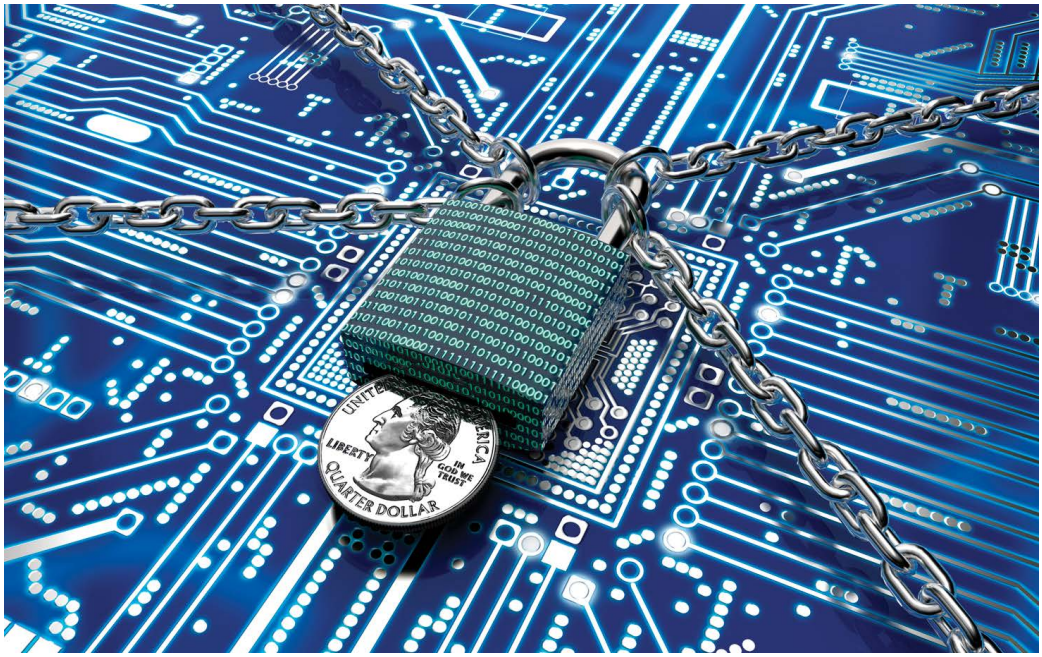
Table of Contents

page

From the individual home user or consumer, to small businesses, up to the largest institutions and government agencies, ransomware is making a widespread impact.

Ransomware and malware have always been a problem, but now fileless malware and ransomware are sweeping through businesses and personal lives as technology becomes more commonplace. Malicious actors, hacktivists, and those seeking to monetize existing vulnerabilities at others' expense are dramatically increasing in numbers. The reason for this is simple, as innovation increases so does the attack surface as well as economic opportunities for attackers. Opportunities for malware implementation are increasing. Malicious tools are available through Malware-as-a-Service (MaaS) or Ransomware-as-a-Service (RaaS) business models, making it easy for anyone—from individuals to large-scale attackers—to start and continue their own malware and ransomware operation.

No one is being spared the effects of ransomware. From the individual home user or consumer, to small businesses, up to the largest institutions and government agencies, ransomware is making a widespread impact. Many of these attacks are delivered through well-known malware kits like Nuclear, Neutrino, and Angler. What is unique; however, is that these attacks include a damaging new encryption stage that shows as cyber extortion. In this stage, critical files, documents, or even the master boot record become locked with enterprise grade encryption, and the attacker is the only one with the key to reverse the process. This key can be obtained with a price, usually in the form of a Bitcoin payment. Where there is money to be made, there you will also find bad actors. The latest abuse, named Cryptojacking, is yet another way for companies and users to be exploited. Rouge scripts are injected into web server code and used to hijack visiting computers processing power to illicitly mint cryptocurrency. While enterprises struggle with how to address these growing attacks, it is up to security software providers to provide an answer.



Ransomware: Relatively New, Unprecedentedly Sophisticated

Ransomware is not entirely new. The first defined case dates to 1989. A biologist distributed 20,000 infected floppy disks to conference attendees at a WHO AIDS conference. The AIDS ransomware creator provided a warning that using the disk would "adversely affect other program applications… and you will owe compensation and possible damages." After this initial attack, ransomware and malware attacks were quiet until 2005 and 2006, when trojans and worms started incorporating an encryption stage into their payloads. In 2011, ransomware type malware made its mainstream debut. As attacker sophistication continued to increase, so did the ability to make this ransomware mimic well-known programs like Windows. With the arrival of CryptoLocker in 2013, ransomware took on a whole new level. The creators leveraged a botnet and peer-to-peer infrastructure. From this initial implementation, it is estimated that they made $5 million in the last four months of the year, with totals estimated to be over $20 million worth of Bitcoin.

Today, there are thousands of variants of malware and ransomware that are distributed through typical phishing, malvertising, and watering hole attacks. They include those more well-known such as CryptoWall, Teslacrypt, Locky, Petya, and WannaCry. Technical professionals are not shying away from the dangers of these, but also expect many more to come. With that expectation comes an increased frustration regarding how to handle current data breaches. With many ransomware and data breaches last year alone, new best practices must be addressed. CSO Online cited experts claiming cybercriminals took in about $1 billion last year, while the FBI has reported $209 million in ransomware payments were made in just the first three months.[1] According to Symantec's Ransomware 2017 report, the U.S. is still the country most affected by ransomware, followed by Japan, Italy, India, Germany, Netherlands, UK, Australia, Russia, and Canada. But outside attacks should not be the only focus.

In 2016, IBM reported that 55% of the cyberattacks faced within a company's framework were carried out by insiders. Before knowledge of insider threats grew, the face of insider threats was fuzzy. Many companies imagined Edward Snowden like characters—a person who worked within the company and whom everyone knew and trusted. Malware and ransomware can present itself in many ways. While the stereotype of a "good employee gone bad" often comes to mind when lingering on this subject, networks can be attacked as simply as by having an employee open an attachment on their email or allow an outside attacker into a company device through an open Wi-Fi network.

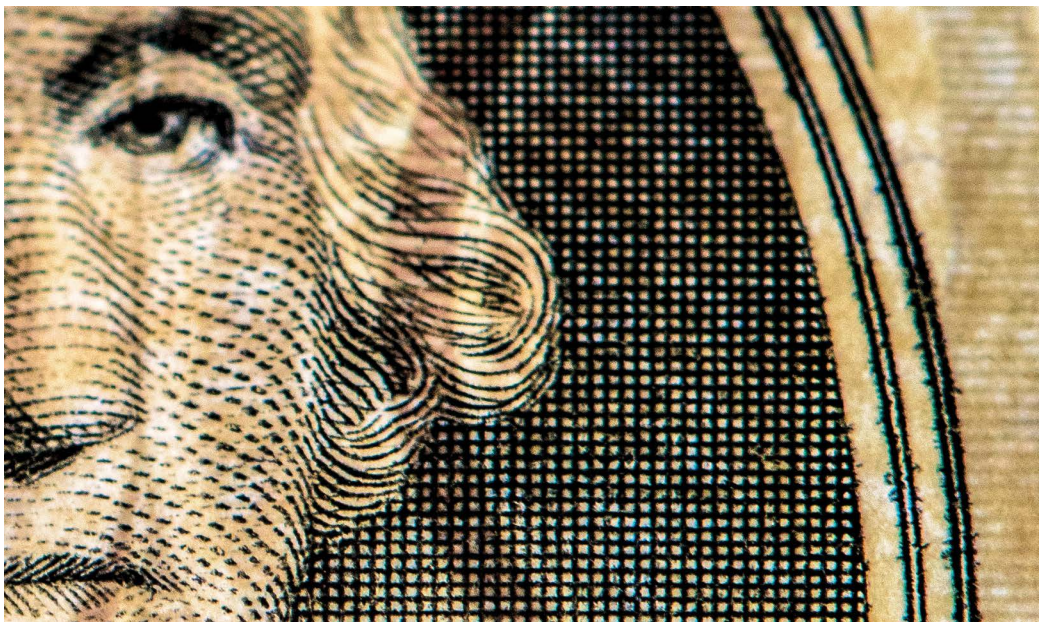
As security professionals, understanding how to accurately address malware and ransomware means understanding how the adversary works and operates. Ransomware is not a consumer-only problem. According to a survey by Radware, 42 percent of companies experienced ransomware attacks, a 40 percent increase from the 2016 survey.[2] The pocketbooks of businesses and institutions are far deeper, and attackers are very aware of this. A multi-layered approach to security is always necessary to ensure that any one failure is mitigated by the defenses of another. Regardless of whether the attack came from

With many ransomware and data breaches last year alone, new best practices must be addressed. CSO Online cited experts claiming cybercriminals took in about $1 billion last year, while the FBI has reported $209 million in ransomware payments were made in just the first three months.

1 **www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html**
2 **www.radware.com/ert-report-2017/**

As security professionals, understanding how to accurately address malware and ransomware means understanding how the adversary works and operates.

the outside or from internally, ransomware and malware is drastically changing the face of companies worldwide and needs to be addressed.



Best Practices: Mitigation, Detection, and Response

Advanced Patching and Having a Patching Plan

Every security plan should start with a well-defined vulnerability and patch management program. Knowing your assets, exposure, and attack surface is critical. You can't rely on informal patching procedures, which are often only completed as time allows. Policy should dictate how current software should be, and how long teams have to patch after new vulnerabilities are discovered. Furthermore, organizations should implement a recurring scan to validate the patch policy is being adhered to. Scans from tools such as NMAP and Nessus can also be integrated into SIEM solutions to provide an up-to-date asset model. ArcSight's ESM, for example, can incorporate this data and use software versioning info and open network ports of systems being attacked in its correlation with attempted exploits, intelligently increasing or decreasing scoring of events of interest. Having an isolated security IDS event, for example, without knowing if the target is vulnerable to a particular attack, increases the time an analyst has to investigate and respond. Having more assets and system data in the SIEM improves the fidelity of the alerts and gets your SOC one step closer to that "single pane of glass" that SIEMs strive to be.

Even without direct integration, much of the data needed to understand an organization's footprint is contained in the event logs being collected. For example, creating a rule to monitor firewall and NetFlow events for any bytes transferred out over port 22 can give you a dynamic list of servers and systems running the SSH service. This can then be provided as a scheduled ArcSight report sent to business units or stakeholders to review, ensuring no ports/services were inadvertently enabled or misused. Taken a step further, perimeter devices are continually being scanned by services like Shodan. The list of Shodan IPs are publicly available, so it would be an easy rule to create that watches all egress/ingress traffic containing a Shodan IP, alerting your organization when new services are discovered by their scanners. Look up the MongoDB massacre of January 2017, for example, where tens of thousands of MongoDB databases left open to the internet were hit by online extortionists. These oversights are easily avoidable with good SIEM content.

Every security plan should start with a well-defined vulnerability and patch management program. Knowing your assets, exposure, and attack surface is critical.

Having Backups

In addition to patch management programs, organizations must perform recurring backups of critical data and these backups must be regularly completed as part of a comprehensive disaster recovery plan. The leverage of ransomware attackers is negated if a recent backup contains most of the crypto-locked files. As could be seen in the attack against Ukraine's federal institutions, when systems are held compromised without a backup, the impact goes far beyond the attacked entity. This is common practice for addressing cyberattacks but should also be done as a regular practice to protect customer information and data loss. That is one way of preparing for the worst, but the best practice also still involves active prevention. Recently, a startling 68% of all data (including funds) lost was declared unrecoverable by those who had undergone attack. Critical information kept by companies needs to be backed up.

User Training

Phishing, Spear Phishing, and Whaling ransomware programs are alive and well. It is still the case that many attacks begin with unwise user behavior. The endpoint is truly the new perimeter, and by extension, so is the end-user. A continuous cyber training program is a must to keep organizations culture of security healthy. This category is so important that Gartner has the Magic Quadrant for Security Awareness Computer-Based Training vendor survey. One consistent leader in the space, PhishMe, understands the benefits that come from integrating their solution into SIEM tools. They partnered with MicroFocus to integrate ArcSight with PhishMe Triage to provide security operations center (SOC) analysts and incident responders insight into ongoing spear-phishing attacks by automating the analysis and orchestrating the workflow associated with employee-reported suspicious emails. Pairing the two platforms together provides enterprise security teams with actionable SIEM workflow automation from human-reported suspicious email and the ability to correlate on event data across the enterprise to take action to remediate threats. Even without such advanced tools, some basic scripting can get you a phishing simulation exercise wherein each email contains a unique URL allowing end-users who clicked to be identified. With these events fed back into ESM, you have a repeatable test that keeps users aware and vigilant.

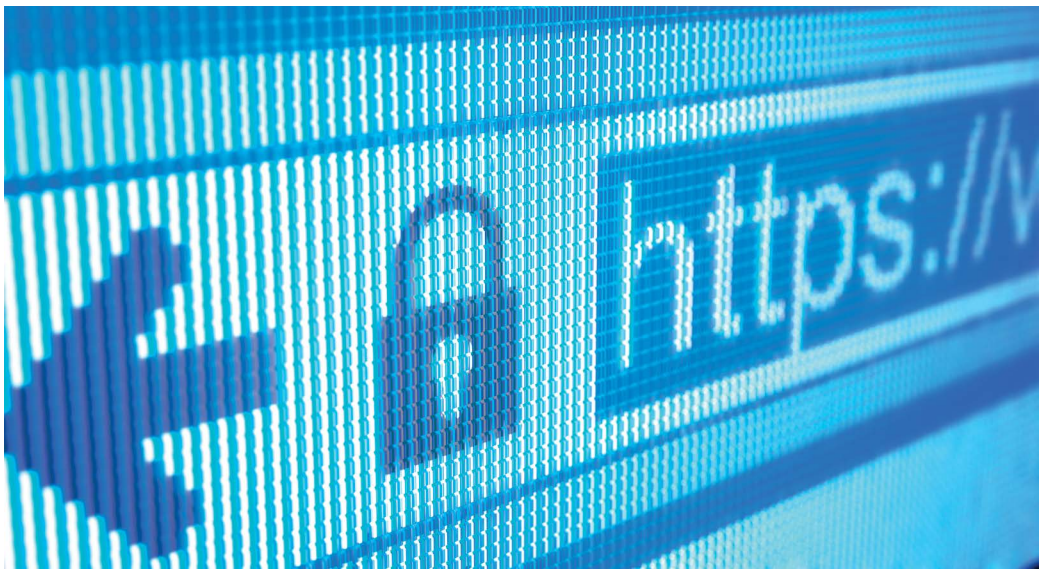
Addressing Visibility Gaps

When it comes to security analytics, more data is usually better. A maturely implemented SIEM has the ability to cut through the noise while still providing analysts with contextual data surrounding events of interest. Achieving this maturity is often easier said than done, but as they say, nothing worth having comes easy. Logging policies should include the following event log types:

- Server & Application Logs
- OS Logs
- Endpoint Security Logs
- Firewall/Proxy Logs and IDS/IPS Logs

Many organizations have large gaps in their visibility due to logs not being collected at one more of these levels. Fortunately, major improvements to event collection technology now make collecting these logs more achievable than before. Windows Event Forwarding used with ArcSight's WiNC, for example, leverages Microsoft's Windows Event Forwarding to centrally aggregate and consolidate events, which are then collected and processed and forwarded to the ESM. WiNC does the heavy lifting of normalizing and parsing any of these Windows event logs and enriches the Windows events with SID and GUID translation. This ensures that the events are not missing important information like which user started a particular process. By using Windows Event Forwarding, you also have the ability to do prefiltering on the event data sources. This conserves bandwidth and enhances connector performance.

For Security Operation Centers that have matured beyond incident response into proactive hunting, MicroFocus partner SOCPrime has some advanced system monitoring rulesets around Sysmon, OSSEC, and OSQuery that integrate with nicely ArcSight ESM. Look here for more info.



User Credential Usage and Living Off the Land

Unlike insider threat, "living off the land" involves a bad actor accessing system credentials to steal data. This is one of the hardest threats to address, as it widely looks like normal activity. It can range from anything like system messages that access employee data to actively logging on and viewing secure system information. The most important way to address living off the land is to not take any action for granted. Allowing automated security tools to process abnormalities while leaving IT personnel to view intra-network processes will help to address this.

Once a "living off the land" event occurs, it is important to program the processes that occurred during that event into prevention software to actively monitor events. Credential use monitoring, Sysmon monitoring, and PowerShell monitoring will also aid in the prevention of this.

The Verizon DBIR report found that 81 percent of data breaches involved weak, default, or stolen passwords. Attackers can evade traditional security monitoring tools as they spread laterally within your environment by using existing tools natively on the system. This is commonly referred to as "living off the land" because attackers are no longer bringing their malicious tools with them, but instead leverage already installed tools like PowerShell, WMI, and PSExec. Fileless ransomware is really gaining popularity. Malicious scripts can be used to write code straight to memory, not having a file on disk to be detected by traditional AV. PowerShell commands are just one of the more popular ways this is achieved.

Network Traffic

Most malware has a command and control (C&C) component. Watching network traffic can sometimes uncover anomalous communications. For instance, SMBv1 Eternal Blue vulnerabilities were used by WannaCry, Petya, and others. Analysts can use SIEM to watch for SMB at the network perimeter including TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139.

Cyber Threat Intelligence (CTI) providers often provide lists of IPs and domains associated with known ransomware that can be used in your SIEMs real-time correlation engine. Threat Intelligence feeds have come a long way and include very granular information on indicators of compromise (IOCs). These IOCs are a great candidate for incorporating into your SIEM solution. Many of the leading threat providers already include prebuilt packages that integrate directly with ESM, such as FireEye iSight, Infoblox IID, EclecticIQ, and Anamoli just to name few. Sharable formats such as STIX/TAXII and YARA allow indicators to be used across tools and platforms. With proper solutions in place, the "dwell time" attackers live within your network will be reduced. Current industry averages still hover near an abysmal 100 days.

Response

When it comes to response, it's all about people, processes, and technology. A good SIEM is key to all three of these areas. SIEM technology really shines with its ability to help organizations triage and respond to threats. Best practices dictate that reportable metrics be created around these processes.

Mean Time to Detection (MTD), Mean Time to Response (MTR) are metrics that can be leveraged begin to track ransomware anomalies. It goes without saying that the longer hackers remain inside your network, the more damage can be done and the harder it will be to remove persistence mechanisms they may have spread throughout your organization. It's an uncomfortable position to be in when your own security team is notified of a breach by an external third party.

A long-held criticism of SIEMs technology is that a SIEM deployment is only as good as its rule-sets and content. MicroFocus has answered this by developing a SIEM best practices called ArcSight Activate based on the Activate Attack Life Cycle and the Activate Defense Monitoring in Depth model. In short, Activate is the methodology for developing and sharing rules and allows for the consistent updating of ESM to keep up with the ever-changing threat landscape.

How ArcSight Works

One of the more exciting areas to follow is the technology in the Orchestration and Automation space. Integrated adaptive cyber defense is the future, and SIEM technology will likely be at the center of many solutions. ArcSight has long had the ability to send scripts to external systems with its CounterAct connector. Adding in more intelligence to automated response solutions will likely appease the fears of false positives and inadvertent system blocks causing outages. ESM 7.0 with its more robust distributed correlation is already positioned centrally in enterprise and adding an automation/orchestration component would be a force multiplier for organizations. Standards are still undefined but look to groups such as OpenC2 to see where things might be headed.

When All Else Fails

Sometimes still, ransomware hits company data and they are further confronted with the question: Should I pay the ransom?

US-CERT has the following guidance: "Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed. NCCIC recommends against paying ransoms; doing so enriches malicious actors while offering no guarantee that the encrypted files will be released."[3]

Assuming the encryption can be reversed, ransomware is still an illegitimate business that should not be acknowledged. By not decrypting data, businesses hurt their own credibility and bottom-line as their business model loses credibility. For the lucky few, the crypto ransomware can sometimes be poorly coded or reverse engineered. In such cases, look to the community for tools to decrypt the files for free, like those hosted at nomoreransom.org. At the end of the day, each organization will have to navigate those waters as they come.

Learn More At
www.microfocus.com/arcsightesm

3 **www.us-cert.gov/ncas/alerts/TA17-132A**

Additional contact information and office locations:
www.microfocus.com

www.microfocus.com