Ransomware Report

Summer 2021 · Volume 1

Secureworks®

Recent headlines have brought new attention to an old problem: ransomware.

We’ve compiled key resources from the Secureworks team of experts to help you stay protected.

Table of Contents

1

Cyber Incident Response Preparation – A Ransomware Use Case

Published: Thursday, June 10, 2021
By: Sophie Bovy - Product Marketing

Summary

- As a leading threat, ransomware presents an important area for incident response preparation
- Incident readiness assessments can be used individually or in tandem to assess ransomware readiness
- Incident response preparation, for ransomware or other threats, benefits from a programmatic approach tailored to an organization's current maturity and objectives

Recent high-profile events continue to reinforce that ransomware is the No.1 cyber threat to organizations today. Last year, our Incident Response team reported a 150% jump in the number of ransomware engagements compared to 2019. This year there are no signs this is slowing down.

A plethora of articles have addressed topical questions about how to best handle and recover from these events. Many are tactical, addressing whether to pay a ransom, for example.

150%

increase in the number of ransomware engagements compared to 2019.

As highlighted in a previous blog by the Secureworks® Counter Threat Unit™ (CTU™), ransomware operators seek to exploit existing systemic network weakness. Our researchers highlight that there are typically two approaches organizations take to prepare for ransomware. The first (and worst) approach is to invest in the latest technologies, expecting a silver bullet. The second is to recognize that 100% prevention is impossible and to take a more proactive approach. This involves seeking to better understand the IT environment, the critical assets that need protecting, and the level of exposure to a potential ransomware attack. The strategy is to master all these elements before it's too late.

One key question to consider:
Are we ready to deal with a potential ransomware incident?

Ransomware Risk Assessments

With that in mind, the initial step for an organization on their ransomware readiness journey is to perform a threat-informed assessment, or Ransomware Risk Analysis. The aim is to document and provide a holistic evaluation of an organization's security controls, processes and technologies across key security domains. Risk ranked findings and recommendations provide the overview that drive a roadmap for remedial action, inform a more pragmatic, prioritized approach to technology investments, as well as help shape an information security risk management process.

Technical Assessments

Complementing a risk assessment with technical assessments helps to highlight additional areas of potential risk and test areas often exploited by ransomware threats. Organizations often choose from one, or all, of the below tests:

- An Active Directory Security Assessment provides insights needed to fix weaknesses in Active Directory misconfigurations, often used by threat actors to distribute ransomware
- A threat hunting assessment can also provide a baseline understanding of threats already present in the environment

- The Secureworks Adversary team offers a Ransomware Resilience Test or Ransomware Simulation Test. This goes beyond automated scanning to mimic the adversary using a hands-on approach modelled using years of offensive experience and the latest threat research. In some cases, after compromise and with a customer's permission, our team can go one step further and execute mock ransomware code for a live simulation to test the response of an organization's blue team. This emulates real-world pre-deployment of ransomware to identify gaps in controls against real TTPs

For a well-rounded IR plan, a follow-up question is needed: Have we practiced enough?

Incident Response Planning and Exercises

Finally, since every second counts during an incident, the key to effective and timely response is proactive incident response preparation. Transforming cyber incident response for readiness and resiliency is a journey that starts with planning, regularly reviewing, and evolving the existing incident response plan and processes.

Incident response preparation starts with planning, documentation, and continues into tabletop exercises. Having a clear objective, such as practicing ransomware readiness, is a requirement for planning an effective tabletop exercise. Tabletop exercises are a first, low-impact step to helping practice a plan.

While frequency of exercises matters to build readiness, it's also important to note that tabletop exercises are just one type of incident response preparation exercise that can be used. Where possible, a robust response program should combine several exercises that leverage mock-ransomware simulations and artifacts, including:

- Functional exercises
- Purple team or full-scale exercises (leveraging live fire simulations as mentioned above)

Practice makes perfect. If you practice with the right inputs and often enough, most of the decisions you need to make during an incident will be made for you, as you've already thoroughly prepared for incident situations.

Programmatic Approach to Incident Response Preparation

No static plan, or single assessment or exercise is enough to keep pace with the evolving threat landscape. Think deliberately and programmatically to build a proactive program that helps improve incident readiness. An organization's existing defenses, current security maturity, objectives and needs should all help dictate what shape incident response preparation should take. Measuring all these elements is a huge task. For this reason, many organizations prefer to get help from outside experts like Secureworks. Look for vendors who take a consultative approach and provide readiness services to build a program of activity that includes assessment, cyber incident response planning and exercises.

Some of our customers feel safest with a Secureworks Incident Management Retainer, which combines advisory and assessment services, workshops and exercises, testing and validation services, plus emergency cyber incident response support. Regular reviews also help organizations continue to mature their IR posture.

2

Prevent the 3 Most Common Ransomware Attack Vectors

Published: Tuesday, June 1, 2021
By: Tony Kirtley – Director, Incident Command

When it comes to ransomware, the basics are an important first line of defense

Summary

- A few basic security controls can greatly reduce your risk of a ransomware attack
- These controls are common and highly effective at preventing ransomware
- Organizations should not wait until they are hit to act

It seems like we hear once a week about a new ransomware victim. What about the ones we don't hear about? Ransomware threat actors are busier than ever and are looking for the easiest payoff possible. Even if your company is in an overlooked industry or doesn't have data that you think would be of particular interest to hackers, you could still be a target.

In the many ransomware engagements to which the Secureworks Incident Response Practice responds, we find striking similarities in the tactics used by threat actors to gain access, move laterally, distribute the ransomware, and finally detonate it. As such, our recommendations for securing networks against such attacks offer a proven standard for ransomware protection.

Initial access vector

The three most common methods that we see threat actors use to gain access to a victim's network are:

1. **Credential Abuse** - Logging in to a remote access gateway via stolen or guessed credentials
2. **Malware Infection** - Installing malware on a host via a phishing campaign or other means
3. **Scan and Exploit** - Exploiting a vulnerability on an Internet-facing server

If you can prevent or detect and block these methods, your risk of follow-on activity is greatly reduced. If the attacker can't get in, what else can they do? The earlier in the process you can stop unauthorized activity, the greater your chances of stopping the attack.

Attackers usually go for the easiest payoff possible

More often than not, this means guessing your credentials and logging in. I'd like to take this opportunity to implore all of you reading this to please, please implement multi-factor authentication on your remote access gateways. The presence of MFA is usually enough to deter the attacker and force them to focus on a less secure organization.

Secondly, many malware infections used for initial entry evade traditional antivirus programs by living only in memory. Cobalt Strike, a tool built for adversary simulations and red team testing, is an example. It is used by penetration testers to compromise networks because it works. However, a good tool with endpoint detection and response capabilities, such as Secureworks® Taegis™ XDR, can detect Cobalt Strike, giving you the advantage over the attacker during the early stages of an attack.

See How Secureworks® Covers MITRE ATT&CK® Framework TTPs and how Taegis XDR maps defenses and countermeasures against more than 90% of all adversarial TTPs used by the malicious software tracked by MITRE.

Lastly, good old vulnerability management is the best way to protect against the Scan and Exploit attack method. Vulnerability management has long been a time-consuming and heavily manual task, but technology is changing this. Secureworks Taegis VDR (Vulnerability Detection and Response) for example, uses AI and analytics to automate much of the manual burden of vulnerability management.

Once they are in

After a threat actor establishes a presence in a victim's network, the activities they perform are fairly predictable. We often see them:

1. Conduct reconnaissance in the network
2. Move laterally
3. Elevate privileges to domain administrator
4. Extract data and destroy backups
5. Distribute and detonate ransomware

Many times, ransomware attackers will conduct these activities using a method called "living off the land," meaning they use the tools that you use to administer the network. Sometimes the attackers use these tools in a way you wouldn't, like encoding PowerShell commands. Detecting and blocking malicious tools and malicious use of authorized tools falls squarely into the job of the tool which handles your endpoint detection and response.

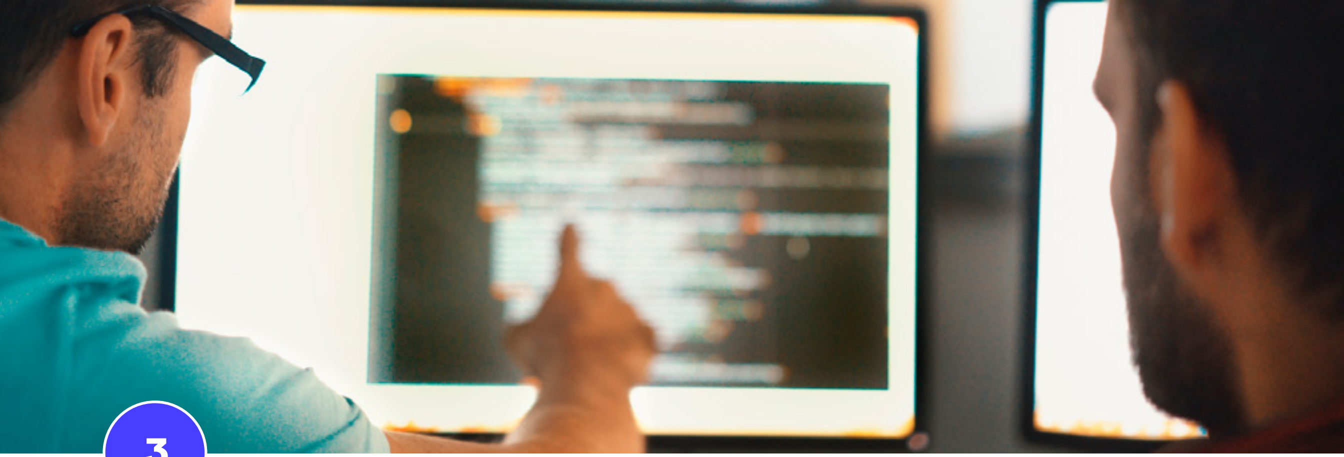
Secureworks Taegis XDR customers often get calls from us when we see this behavior, indicating that ransomware is coming. Our incident responders spring into action to guide the victim through the steps to evict the threat actor from the estate in a timely fashion.

Other controls that can help make it harder to compromise your network include strengthening the security of your Active Directory. Without privileges, it is harder to perform the malicious activities in the kill chain. Our Active Directory Security Assessment is an incident readiness service available with the Incident Management Retainer that can help you with this.

Lastly, we have seen threat actors who have compromised a victim's network divert their attention elsewhere upon discovering that they cannot destroy the victim's backups. Think about it: If you were trying to make money, would you waste your time with a company that had the means to recover data without paying you? I think not. It pays to store your backups off-line.

One final thought

And as always, logging to a central collection facility is going to be key in detecting badness in your network. Our Taegis XDR security operations and analytics platform allows you to send as many infrastructure log types as you want at no additional cost, giving Secureworks the ability to apply our intelligence, correlate infrastructure logs with endpoint logs, and enable threat hunting and incident response, all in the same program.



3

Ransomware Prevention, the White House, and a Risk-Based Vulnerability Management Approach

Published: Thursday, June 24, 2021

By: Shaun Donaldson - Product Marketing

Ransomware and other cyberattacks are a massive problem – recently attracting the attention of the White House. New vulnerability management technology offers a way to identify vulnerabilities and quantify risk, so you can act fast to close gaps and keep threat actors out.

Summary

- Ransomware prevention is a massive challenge and has gained considerable attention
- Focus on risk-based vulnerability management as key line of defense against threat actors
- New technologies offer critical improvements over legacy vulnerability management strategies

The Global Impact of Ransomware is Surging

Ransomware has a long history, going back to 1989. The grift is straightforward. First, deliver a malicious payload which disrupts an organization by encrypting data in such a way that only the attacker can provide decryption. Second, extort the organization for payment in exchange for (if there is honor amongst thieves) what is needed for decryption and/or not releasing sensitive data.

There have been multiple waves, and they seem to get worse with each iteration. WannaCry was a particularly widespread attack which leveraged the EternalBlue exploit kit, leaked by the Shadow Brokers outfit. WannaCry was followed by NotPetya, which also used EternalBlue.

The latest wave has garnered a lot of attention. The Colonial Pipeline attack had an impact on not just the company, but on consumers in the United States as operations at one of the largest pipeline operators in the country were interrupted before the company paid the ransom. A large meat supplier was also recently butchered by an attack which impacted their operations.

This spate of high-profile attacks in recent years has made cybersecurity and ransomware familiar topics to the general public. This has lifted ransomware prevention from an IT security issue to something a wide swath of the population is aware of and impacted by. Some of those paying a lot more attention to the problem have quite a bit of influence. Recent attacks likely spurred a May 2021 Presidential executive order which offered recommendations on improving cybersecurity for the United States federal government, and a later memo from the White House which offered advice to private organizations.

Risk-Based Vulnerability Management Output Is a Challenge

The recent White House memo identified risk-based patch and vulnerability management as a priority for organizations. A robust vulnerability management program is an important line of defense against ransomware attacks. An open vulnerability is an opportunity for a threat actor looking to deploy ransomware. But vulnerability management is often a tricky, time-consuming, and highly manual task. Vulnerabilities are so numerous organizations often don't know which to patch first. This leads to many security teams relying on blanket vulnerability severity scores to identify which to address first. But just because a vulnerability has a high severity score, that doesn't mean a company your size, in your vertical, with your unique security setup is at risk. It can't be overstated: context is key in vulnerability management.

There are gaps that grow into chasms in the process of assessing risk to guide vulnerability remediation efforts. It starts with understanding where your assets are across highly dynamic multi and hybrid-cloud environments, probing to understand the vulnerabilities those systems and web applications have, transforming vulnerability data into actionable information based on risk, which finally leads to where you can best focus remediation.

Moving through the process with traditional tools requires a lot of time-consuming manual effort, which increases the chances of gaps and mistakes. It is also prone to errors, missed assets, overly simple prioritization, somebody being on vacation... the list is long.

How to Ease the Burden of Identifying Vulnerabilities and Quantifying Risk

The White House memo identified the right approach toward vulnerability management, but it didn't set out a plan for how to get there. A tip for all organizations who want to achieve their vulnerability management goals: Forget the old ways of doing things – the latest vulnerability management products provide powerful automatic vulnerability contextualization, removing confusion and manual error in the process.

We are living in an era where vulnerability management products can:

- Discover assets across the entire enterprise (physical, virtual, IoT, on-premises, cloud, web applications)
- Assess the vulnerabilities present from both an external and internal viewpoint

- Prioritize the vulnerabilities based on risk by using artificial intelligence and machine learning that takes both external and internal factors into account

- Produce a ranking of all vulnerabilities, based on risk, to guide remediation efforts

These capabilities reduce the burden of vulnerability management and allow a precision of action which was previously very difficult to achieve. Modern vulnerability management products can automatically scan for assets and probe endpoints and web applications to identify vulnerabilities, while also assessing risk based on factors relevant to an organization. But often, the value they provide goes much deeper than this.

Let's take Taegis™ Vulnerability Detection and Response (VDR) as an example. A simple way of understanding the power this technology offers is this: Imagine VDR is like having 40+ experts dedicated to providing data to your vulnerability program, all day every day. One expert is focused on the availability of remote exploits of each vulnerability, another is researching threat actor chatter on the dark web to see how threat behavior relates to vulnerabilities. Another expert is focused on the position and criticality of each asset relative to other assets, while a different person researches intelligence about threat actors from trusted sources. Continue this thought experiment for a further 36 or so factors critical to vulnerability management and you have a picture of how VDR works. This kind of automated vulnerability identification and categorization can help organizations achieve what seem like lofty and arduous goals for their program. Through swift and accurate identification of vulnerabilities, the risk of ransomware is significantly reduced.

So while the recommendations from the White House seem difficult to achieve in practice, in reality new technologies like VDR simplify the process and make it much more effective.

See for yourself with a Taegis VDR Demo.

4

Stop Ransomware With Taegis

Protect your organization from ransomware with Secureworks Taegis™ Security Operations and Analytics Platform. Taegis brings together extended detection and response (Taegis XDR or Taegis ManagedXDR), vulnerability management (Taegis VDR), and continuously curated, comprehensive threat intelligence to help you reduce the risk of a ransomware attack and stop ransomware prior to data exfiltration and file encryption.

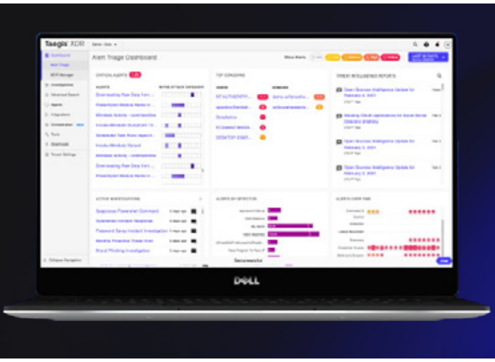
Even though ransomware perpetrators are numerous and their profiles diverse, you can get an early warning about emerging ransomware campaigns by leveraging the original research by the Secureworks Counter Threat Unit™ (CTU) covering APTs, criminal groups, ransomware-as-a-service providers, and other threat actors. For example, in 2020 and 2021, CTU™ discovered and analyzed Darkside and Snatch ransomware operations' use of the Tor client to create a backdoor with persistent access to compromised networks via Remote Desktop Protocol (RDP). With information like this, available at no extra charge to Taegis customers, you can mitigate exposure to ransomware by following CTU researchers' recommendations. Further, CTU research, alongside added Incident Response and Adversary Group insights, drives continuous enhancement of Taegis countermeasures, advancing its capacity to detect new threats.

Taegis Extended Detection and Response (XDR)

Unified Detection and Response

Gain holistic visibility and control over your endpoint, network, and cloud environments. Detect and respond to advanced threats with AI-driven analytics and curated comprehensive threat intelligence.

Try Taegis XDR



Taegis Vulnerability Detection and Response (VDR)

Simplify Vulnerability Management

Identify and remediate the most critical vulnerabilities with contextual prioritization and an automated, configuration-free approach.

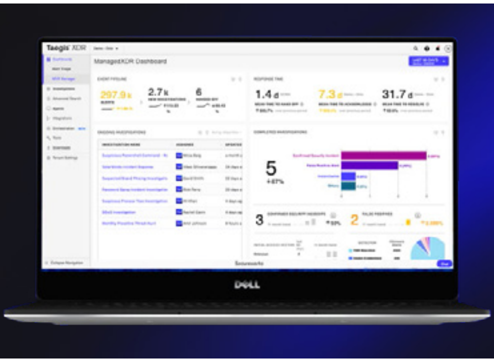
See a Demo

Taegis ManagedXDR

Intelligent XDR Multiplied by Deep Expertise

Multiply the detection and response capabilities of Taegis XDR by the elite security expertise of Secureworks analysts. Realize up to a 413% ROI as Taegis XDR relentlessly scours your telemetry around the clock for signs of threat activity and our experts respond and remediate quickly.

Learn More



About Secureworks
Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

For more information, including threat intelligence, advisories and practical advice, **visit our Ransomware webpage.**