Ransomware Preparedness: A Call to Action

crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/

Josh Dalman - Kamil Janton - Eben Kaplan April 27, 2021

Hardly a day passes without news of another company, hospital, school district or municipal government temporarily brought to a halt by ransomware. In fact, ransomware attacks have become so commonplace that they make the news far less than they used to.

Yet while ransomware may no longer captivate the public's attention, security professionals justifiably continue to obsess over it. Ransomware remains the most profitable method for cybercriminals to monetize their unauthorized access into business networks, with increasing ransom demands often ranging from $1 million to $10 million USD. For this reason alone, all organizations are potential targets for ransomware campaigns that almost always have a costly business impact, including disruption to operations and extortion that involves sensitive data theft.

Ransomware preparedness has become imperative for all organizations, so much so that even chief executives and boards of directors are recognizing it as part of their responsibility to promote good governance. But it is a cat-and-mouse game — as defenses improve, ransomware actors continue to innovate to find new methods to compromise and extort their victims.

The CrowdStrike® Services team routinely assists organizations both in preparing for and responding to ransomware attacks. The following are some of the practices we recommend most frequently.

Improve Resiliency of Internet-facing Applications

CrowdStrike has observed eCrime threat actors exploiting single-factor authentication and unpatched internet-facing applications. BOSS SPIDER, one of the initial big game hunting (BGH) ransomware threat actors, routinely targeted systems with Remote Desktop Protocol (RDP) accessible from the internet. Less sophisticated threat actors operating ransomware variants such as Dharma, Phobos and GlobeImposter frequently gain access through RDP brute-force attacks.

CrowdStrike recommends against RDP being exposed directly to the internet. Organizations currently leveraging the CrowdStrike Falcon® platform can quickly and effectively identify systems being actively brute-forced via RDP by using the following query in the Falcon Event Activity Monitor:

```
event_simpleName=UserLogonFailed2 | iplocation RemoteAddressIP4 | stats
values(ClientComputerName) AS ClientComputerNames dc(UserName) values(LogonDomain) AS
LogonDomains dc(RemoteAddressIP4) values(LogonType_decimal) dc(Country) count by
event_simpleName ComputerName | sort -"dc(Country)"
```

In a separate but similar campaign in 2020, CrowdStrike observed CIRCUS SPIDER, the group behind the development of Netwalker ransomware, and TWISTED SPIDER, the group behind the development of Maze ransomware, exploit CVEs (common vulnerabilities and exposures) associated with Pulse VPN to gain access into victim organizations. For this reason, CrowdStrike recommends utilizing a VPN with multifactor authentication, and ensuring that any CVEs associated with the VPN platform(s) and the underlying authentication application are prioritized for patching. This principle should extend to all remote methods including, but not limited to Azure Active Directory (AD) and Citrix Gateway. The latter, being used by threat actors such as TRAVELING SPIDER — the criminal developer of Nemty ransomware — has been observed by CrowdStrike to take advantage of single-factor authentication to gain access to victim organizations through Citrix Gateway and send extortion-related emails using the victim's own Microsoft Office 365 instance.

Implement and Enhance Email Security

Gaining an initial foothold into a victim organization through a phishing email is the most common tactic for BGH ransomware groups. Typically, these phishing emails contain a malicious link or URL that delivers a payload to the recipient's workstation.

CrowdStrike recommends implementing an email security solution that conducts URL filtering and also attachment sandboxing. To streamline these efforts, an automated response capability can be used to allow for retroactive quarantining of delivered emails

before the user interacts with them. In addition, organizations may want to restrict users from receiving password-protected zip files, executables, javascripts or Windows installer package files unless there is a legitimate business need. Adding an “[External]” tag to emails originating from outside of the organization and a warning message on top of the email’s body can help remind users to use discretion when handling such emails.

Users should also have a documented process to report any emails they are unsure of along the way. In addition, if business permits, organizations should consider restricting users’ access to personal email accounts.

As always, organizations should also implement a robust security awareness program that includes routine user training, reminders and “phish-me” campaigns. Creating your own “phish-me” campaign is one of the best and safest ways for your employees to learn to not be fooled by phishing emails. The old adage applies: “Fool me once, shame on you — fool me twice, shame on me.” CrowdStrike employs this best practice internally.

Harden Endpoints

Throughout an attack lifecycle that ultimately culminates in a ransomware deployment, threat actors will often leverage a number of endpoint exploitation techniques. These exploitation techniques vary from exploiting poor AD configurations to leveraging publicly available exploits against unpatched systems or applications.

A proper endpoint hardening strategy will ensure that threat actors have to defeat multiple defensive layers before achieving success in the attack. Each layer of defense the threat actor encounters provides an opportunity for defensive teams to detect and ultimately contain the activity before it results in ransomware deployment.

The list below includes some key system-hardening actions for defenders to implement. It is important to note this is not an exhaustive list, and system hardening should be an iterative process.

- **Ensure full coverage across all endpoints on your network for endpoint security products,** and for the endpoint detection and protection (EDR) platform. Each endpoint security platform should have strict anti-tampering protections and alerting in place if and when a sensor goes offline or gets uninstalled.
- **Develop a vulnerability and patch management program.** Doing so will ensure that all endpoint applications and operating systems are kept up-to-date. Ransomware actors leverage endpoint vulnerabilities for many purposes, including but not limited to privilege escalation and lateral movement. Existing Falcon customers can leverage CrowdStrike Falcon Spotlight™ vulnerability management for a near real-time way to understand exposure to a particular vulnerability across the environment, without the need to deploy additional agents and security tools.

- **Follow Active Directory security best practices.** Based on some of the most common AD downfalls observed by CrowdStrike Services during ransomware engagements, we recommend these steps:
    - Avoid easy-to-guess passwords with weak authentication methods.
    - Avoid having regular domain users with local administrator privileges, and local administrator accounts with the same passwords across the entire enterprise or large portions of the enterprise.
    - Limit workstation-to-workstation communication. While this can be achieved using group policy objects (GPOs), it can be also achieved through a number of micro-segmentation software options.
    - Avoid sharing privileged credentials. Poor security practices include shared administrative accounts and using administrator accounts for personal or day-to-day business activity that does not require administrator privileges.
    - Note that the first two points above can be accomplished using AD with little to no additional costs. At an additional cost, a privileged access management (PAM) solution can provide a much more scalable and robust solution to the same problem and is discussed more later in this blog post.

With the recent acquisition of Preempt, CrowdStrike is continuously adding capabilities to its Zero Trust framework. The “Implement an Identity and Access Management (IAM)” section of this blog explains how Falcon Zero Trust can help you further harden your endpoints and improve your IAM program.

Ransomware-proof Data with Offline Backups

In recent years, and since the emergence of ransomware as a top method of monetizing attacks, the developers behind malicious code have become very effective at ensuring victims and security researchers cannot decrypt affected data without paying the ransom for the decryption key. Further, when developing a ransomware-proof backup infrastructure, the most important idea to consider is that threat actors have targeted online backups before deploying ransomware to the environment.

For these reasons, the only sure way of salvaging data during a ransomware attack is through ransomware-proof backups. For example, maintaining offline backups of your data allows for a quicker recovery in emergencies. The following points should be considered when developing a ransomware-proof offline backup infrastructure:

- Offline backups, as well as the indexes (describing which volumes contain which data) should be completely separate from the rest of the infrastructure.
- Access to such networks should be controlled via strict access control lists (ACLs), and all authentications should be performed using multifactor authentication (MFA).

- Administrators with access to both offline and online infrastructures should avoid reusing account passwords and use a jump box when accessing the offline backup infrastructure.
- Cloud storage services, with strict ACLs and rules, can also serve as offline backup infrastructure.
- Emergency situations such as a ransomware attack should be the only time the offline infrastructure is allowed a connection to the live network.

Restrict Access to Virtualization Management Infrastructure

As mentioned earlier, threat actors engaged in big game hunting ransomware campaigns are continuously innovating to increase the effectiveness of their attacks. The most recent such development includes the ability to attack virtualized infrastructure directly. This approach allows for targeting of hypervisors that deploy and store virtual machines (VMDK). As a result, the endpoint security products installed on the virtualized machines are blind to malicious actions taken on the hypervisor.

To further understand how this attack would unfold, we will use some of VMware's naming convention as it is the most common virtualizing product found in today's enterprise environments.

Many ESXi systems (VMware hypervisors) do not have Secure Shell (SSH) protocol enabled by default and are usually managed via vCenter. If SSH is disabled, previously stolen administrative credentials are used to enable SSH on all ESXi systems. Once that is complete, a valid account is used to SSH into each ESXi system being targeted. Before the threat actor deploys the Linux-based ransomware, VMDKs hosted on the ESXi are stopped to allow the ransomware binary to access the files for encryption purposes. Systems impacted by the ransomware through this deployment method will be completely offline and inaccessible to the users.

Recently, CrowdStrike Intelligence has observed this method being used by CARBON SPIDER and SPRITE SPIDER, and CrowdStrike expects this trend to continue to be used and adopted by eCrime operators. As adoption of this tactic becomes wider, the following items can help organizations strengthen their virtualized environments.

- Restrict access to ESXi hosts to a small number of systems, and ensure these systems are fully patched and have proper endpoint monitoring in place.
- ESXi systems are commonly managed via LDAP-binded Active Directory accounts, which are often privileged accounts targeted by the threat actor earlier in the compromise. Removing or limiting such bindings could minimize the chance of an already-compromised administrative account being used to target the ESXi systems with ransomware.
- Ensure SSH access is disabled, or ensure that it is secured by MFA.

- Ensure passwords are unique to each ESXi host as well as to the web client and are strong/complex, using a combination of letters, special characters and numbers. Avoid using dictionary words and “1337” speak.
- Enable Normal Lockdown Mode to further restrict access. See reference here.

Implement an Identity and Access Management (IAM) Program

Organizations can improve their security posture by implementing a robust IAM program that maintains an activity trail for all privileged and service accounts, with immediate identification for anomalous traffic or abnormal resource requests.

To help organizations implement an IAM program, CrowdStrike offers two Identity Protection modules: Falcon Zero Trust and Falcon Identity Threat Detection. Deploying these modules to an existing Falcon instance will create real-time layers of threat prevention of identity-based attacks and anomalies targeting an organization. The adaptive capabilities of this platform allow enterprises to automate responses with the right type of enforcement or notification based on identity, behavior and risk. For example, service accounts attempting to connect via RDP, or RDP connecting to an unusual destination, could be challenged via multifactor authentication or blocked by Falcon Zero Trust in real time.

In addition, nearly all BGH ransomware groups will utilize off-the-shelf credential dumping tools such as Mimikatz or SPRITE SPIDER’s PyXie and LaZagne modules to steal credentials and expand their foothold within the environment. The output of the tools are then used by the attackers to move laterally within a network using techniques such as Pass-the-Hash, Pass-the-Ticket, Kerberoasting and others.

An IAM platform such as Falcon Identity Protection can detect credential exploitation as well as the use of risky protocols and abnormal behavior within the AD environment. These detections will identify devices and accounts that have been compromised and, based on the configured policy, decide if such accounts need to be challenged via MFA/2FA or blocked to halt the progress of the attack. This will significantly cripple BGH ransomware groups from being able to act on their objectives.

Develop and Pressure-test an Incident Response Plan

Organizations sometimes become aware of threat actor activity within their environment, but they lack the visibility to address the problem or the right intelligence to understand the nature of the threat. Recognizing the threat and responding quickly and effectively can be the difference between a major incident and a near miss.

Incident response plans and playbooks help facilitate that speedy decision making. Plans should cover all parts of the response effort, across the organization. For the security team, they should provide aids to decision-making so that front-line responders don’t overlook

important details while triaging alerts. They should also outline the extent of the security team's authority to take decisive actions — such as shutting down business-essential services — if a ransomware attack appears imminent.

For the crisis management team, plans should identify who will be involved and what their roles and responsibilities are. It should also tee up important decisions, like when to activate an incident response retainer, whether to notify insurance carriers, when and how to involve in-house or outside counsel, and how to discuss ransom demands with executives.

Consider conducting regular tabletop exercises to test the incident response plan and processes. Some organizations may benefit from simulated exercises such as "purple team" engagements, where red teamers mimic ransomware operators' actions on objectives, including data exfiltration and ultimately ransomware deployment. CrowdStrike also recommends regular exercising of your incident response plan, both planned and unplanned, such as utilizing a red team to conduct a mock attack operation.

Organizations should never be surprised or caught flat-footed by an attack — it should be expected and planned for.

Take Steps Now

Any organization can fall victim to costly ransomware campaigns with ransom demands in the seven digits, but much can be done to stop threat actors before they get a chance to detonate a widespread ransomware attack. Locking down common initial entry vectors, implementing multifactor authentication, and hardening of both endpoint and Active Directory infrastructure can pay dividends by improving an organization's resiliency to ransomware threat actors.

While it's not possible to prevent all network intrusions, creating enough obstacles through principles of security-in-depth, and the recommended "1-10-60" benchmark time (one minute to detect an incident, 10 minutes to investigate and one hour to remediate), can ensure that threat actors are halted before achieving their objectives of data theft and ransomware deployment.

Additional Resources

- *Learn about recent intrusion trends, adversary tactics and highlights of notable intrusions in the CrowdStrike 2021 Global Threat Report.*
- *Understand the trends and themes that we observed while responding to and remediating incidents around the globe in 2020 — download the latest CrowdStrike Services Cyber Front Lines Report.*
- *Learn more about the CrowdStrike Falcon® platform by visiting the product webpage.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*