Addressing Ransomware Attacks and Other Malware

Use visibility, control and orchestration to reduce your attack surface and unify response

The recent wave of ransomware attacks has raised concerns about serious vulnerabilities in enterprise networks. Ransomware was the top attack vector in 2016 for the Financial industry[1], and attacks on Healthcare organizations are on the rise, with hospitals being primary ransomware targets[2]. At ForeScout Technologies, we offer unique security solutions that can help detect unauthorized or malware-infected devices, control their actions and orchestrate rapid and effective responses to cyberattacks.

The Challenge

The notorious "WannaCry" ransomware was unleashed in May 2017 in a massive attack that targeted hundreds of thousands of users across multiple industries in close to 150 countries.[3] This ransomware locked up computers in car factories, hospitals, retail shops and schools.[3 4] Users were confronted with a screen demanding payment to restore their files.[3 4]

Ransomware attacks are nothing new. Many organizations have been on the receiving end of these types of attacks for years. In some cases, organizations have actually paid ransoms of tens of thousands of dollars to get their operations back up and running quickly.[5 6] But more than the ransom amount, it is the operational impact that takes a bigger toll on organizations.

WannaCry exploited a vulnerability in the Windows Server Message Block (SMB) protocol. Microsoft had patched the vulnerability, but since it affects older, as well as newer, versions of Windows, getting everybody to upgrade is a challenge. There are still many people and organizations that don't regularly patch their systems. Some don't install patches because they don't have strict policies to keep their systems up to date; others don't install patches because upgrading to the latest software may have a sizable operational impact. In addition many organizations use expensive operational technology devices, such as medical and manufacturing equipment, that rely on custom software built on older versions of the Windows operating system, including Windows XP.

The rapid adoption of the Internet of Things (IoT) adds another huge layer to the global list of vulnerabilities. IoT adoption will continue to grow rapidly because the benefits are quite compelling. However, many IoT devices are extremely vulnerable to attacks since they cannot host third-party security agents, run outdated or unsupported software, cannot be patched and often lack even the most basic security features. These devices increase the attack surface for ransomware and other malware.

In fact, IoT-related ransomware attacks are already happening. According to *The Local*, an Austrian newspaper, a ski resort in Austria was hit by a ransomware that resulted in all its guests being locked out of their rooms, while also shutting down the hotel's entire computer system.[6] The hotel had to pay thousands in bitcoin ransom to cybercriminals to get the rooms unlocked, and, unbeknownst to the staff, the hackers had built in a backdoor to their fix, which resulted in two more ransomware attacks.[6] Another high-profile attack occurred in the days preceding the U.S. presidential inauguration in January 2017, causing the Washington D.C. police force to scramble to clear a ransomware infestation from its CCTV camera servers.[7]

To prevent and combat such attacks, it is critical to have attack prevention, detection and remediation strategies work in tandem across the network. An agentless, network-based security system is critical to effectively see, control and orchestrate a system-wide threat response. This is where ForeScout can help.

Blocking USB Drives

Many companies—and some entire industries—forbid the use of removable drives. In addition to the obvious risks of data theft, removable drives can introduce ransomware and other malware onto the network.

CounterACT provides control of USB drives on Windows® systems.* Using its policy template wizard, you can build a policy to detect and classify hosts that have these external device types connected to them:

- Wireless communication devices
- Windows portable devices
- Windows CE USB devices
- Printers
- PCMCIA and flash memory devices

Other devices:

- Network adapters
- Modems
- Infrared devices
- Imaging devices
- Disk drives
- DVD/CD-ROM drives
- Bluetooth radios

Next, simply apply the desired action to the policy to disable these devices' USB ports. The devices remain blocked until the action is cancelled, even if the device is inserted, removed and later reinserted.

* Requires the use of SecureConnector™, which can be automatically installed upon deploying actions.

The ForeScout Solution

ForeScout is uniquely positioned to reduce ransomware and other malware-related risks for businesses and government organizations in three distinct ways:

See ForeScout CounterACT® offers the unique ability to see devices the instant they connect to your network, without requiring software agents or previous device knowledge. Agent-based solutions are blind to unmanaged endpoints and many IoT devices. Periodic security (in contrast to continuous security) creates large gaps in visibility. In addition to discovering endpoints using agentless visibility, CounterACT helps you quickly classify and assess them, and continuously monitors the devices as they drop on and off the network. Visibility is very important because you can't secure what you can't see. A study done by IDC showed that, after deploying the ForeScout platform, on average, ForeScout customers saw 24 percent more devices on their networks.[8]

Control CounterACT enables a broad range of network access controls. Many security tools lack remediation capabilities for systems with missing, broken or misconfigured agents. But with the ForeScout platform, you can automate control actions that allow, limit or deny network access based on device posture and your security policies. In addition, the ForeScout platform lets you automatically quarantine, remediate or block non-compliant or compromised devices—all without manual intervention. Also, should you choose to isolate specific devices to a particular network segment or VLAN, CounterACT simplifies this process.

Incidentally, the WannaCry ransomware attack took advantage of a vulnerability in the Server Message Block (SMB) protocol. CounterACT can be used to disable SMB at the network level for all boundary devices. However, operational impacts should be considered before taking this action, as some systems may be dependent on these ports being open.

Orchestrate ForeScout's ability to tear down security management silos through system-wide threat response orchestration dramatically enhances network security. Orchestration begins with CounterACT's broad interoperability with third-party network and management systems and ForeScout's commitment to share security insights with them. Through ForeScout Extended Modules, we extend CounterACT's agentless visibility and control capabilities to leading solutions for Advanced Threat Detection (ATD), Enterprise Mobility Management (EMM), Vulnerability Assessment (VA), Next Generation Fire Wall (NGFW), Security Information and Event Management (SIEM), Endpoint Protection Platform (EPP) and Information Technology Service Management (ITSM).[9]

Specific examples include:

- EPPs require functional endpoint agents and current antimalware signatures. When an endpoint connects to the network, CounterACT can scan for a functional and current antivirus client as well as patch level and updates as required for compliance with your security policies. If a device has a missing or broken agent, CounterACT can inform the EPP to install/repair the agent and offers capabilities to assist in remediation.

- As with any security incident, time is of the essence. If the exact makeup of the ransomware is not known, as is typically the case with zero-day exploits, CounterACT can leverage bi-directional information-sharing with your ATD and VA systems to automate policy-based security actions in real time.
- CounterACT can block communication to a ransomware's Command & Control server if the Indicator of Compromise (IOC) is known. Malicious IP addresses may change on a minute-by-minute basis. This is where an ATD comes in. CounterACT can receive updates regarding IOCs from popular ATD products and use them to block data and collect the information.
- The ForeScout platform can initiate on-demand VA scans, identify the vulnerabilities exploited by ransomware and work diligently with your VA systems to address them.
- CounterACT can alert the Security Operations Center (SOC) as to indications of a security threat and risk level with information obtained from the SIEM platform. If needed, CounterACT can also handle incident response by taking action on devices based on correlations and feeds coming into the SIEM system.

CounterACT can also isolate infected endpoints, kill malicious processes or initiate other remediation actions. In addition, it can see suspicious traffic and control it, block it altogether or issue an alert on it.

Addressing the Ransomware Threat

Ransomware attacks can be prevented through effective security management and training. Although the following best practices are recommended specifically to prevent ransomware attacks, the same security principles, processes and solution components apply to effectively mitigate risks posed by other types of malware.

1) **Educate the employees:** Employees should be made aware of unsafe work practices. Ransomware typically gets into the network through employee actions such as opening attachments from phishing emails, downloading malicious documents, browsing infected websites, clicking on malicious links or copying malicious files from an infected USB. System administrators should be trained to make sure that employees have access only to those parts of the network and assets that are needed for their work.
2) **Back up the data:** Scheduling regular backups is a good way to avoid ransom demands. But keep in mind that re-imaging systems to get them up and running again will still have a considerable operational impact.
3) **Stay up to date with patches:** The lesson from the WannaCry attack is obvious: keep your system patches up to date. Ransomware protection requires keeping managed endpoints on your network properly configured, patched and current with regard to security safeguards. Automate processes to keep the machines up to date with the latest patches. If the systems cannot be patched to the latest version for operational reasons, protect them by placing them in separate network segments.
4) **Proactively protect against attacks:** In addition to all these steps, it is important to have an effective security solution in place that can anticipate and prevent an attack. However, in the event that an attack gets through all of your defenses, the solution should be able to effectively respond, contain and remediate issues. A security system that can see, control and orchestrate system-wide threat response can help achieve this.

Addressing the WannaCry Vulnerability

Microsoft published patches to resolve the SMB vulnerability for supported Windows versions on March 14, 2017 (Microsoft Security Bulletin MS17-010). The CounterACT publication, HPS vulnerability DB 17.0.3, released on March 20, 2017, includes this vulnerability update.

ForeScout has security policy templates that can help to quickly identify and mitigate WannaCry ransomware. The policy templates content plugin includes templates to identify:

- WannaCry-vulnerable endpoints
- WannaCry-infected endpoints

Organizations can create policies using these templates and add actions to mitigate the risk from vulnerable and infected endpoints. These templates also include support for Windows versions that are no longer officially supported by Microsoft: Windows XP, Windows 8 and Windows Server 2003.

ForeScout CounterACT can update the endpoints with the appropriate patch by using native Windows domain policies or by leveraging third-party EPP agents from McAfee, FireEye and Symantec. If needed, the ForeScout platform can also help block ports that are vulnerable (TCP 445 used for SMB, ports 137-139 used for NetBIOS) for all boundary devices. ForeScout can also work with third-party systems to update antivirus and keep them up to date.

As an additional layer of security, vulnerable endpoints—especially ones running older Windows versions—can be placed on restricted network segments so access is limited.

Learn more at
www.ForeScout.com

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

[1] https://www.forescout.com/sans-2016-survey-on-security-and-risk-in-the-financial-sector/

[2] http://fortune.com/2017/05/15/ransomware-attack-healthcare/

[3] http://www.cnbc.com/2017/05/14/cyber-attack-hits-200000-in-at-least-150-countries-europol.html

[4] http://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday

[5] http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[6] https://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms

[7] https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.3561a4087e7b

[8] https://www.forescout.com/idc-business-value/

[9] https://www.forescout.com/products/extended-modules/orchestrate/