UNISYS | Securing Your Tomorrow®

5 Ways to Deliver A Deadly Counterpunch to #Ransomware.

By Mat Newfield and Prof. Sally Eaves

Ransomware is a specific type of malware designed to encrypt a computer's content until the user pays to get the recovery key.

With phishing sites growing by 640% in 2019[1], 65% of ransomware attacks delivered via phishing[2] and 90% of corporate data breaches being caused by human error[3], the threat of ransomware hangs over every IT professional. The average cost of a breach ranges from $5.11 million for large organizations to $2.65 million for smaller organizations. The global cost to victims of ransomware is estimated to be $20 billion in 2020.

Ransomware is a specific type of malware designed to encrypt a computer's content until the user pays to get the recovery key. This effectively halts productivity, impacting business revenue. However, IT professionals can take decisive action to minimize both the threat and the impact of ransomware. Here, we define the preventative steps that can be taken to protect the enterprise against ransomware, examine how to limit the impact of a breach, explore where an in-process attack can be stopped, and discuss what to do if a hacker succeeds in gaining access.

1. Protect the Enterprise

The first line of defense is always a good offense. To prevent an attacker from establishing a foothold in your organization's network, be sure to put in place the following:

- **Develop a Ransomware Plan** so you will be prepared to respond rapidly.
- **Follow best practices** such as strong vulnerability management and patching policies, regular system backups, Multifactor Authentication (MFA), restrictions of local administrator rights and privileges.
- **Encourage, train, and periodically retrain users** to:
  - Never click on links or open attachments in unsolicited emails.
  - Back up data on a regular basis. Keep it on a separate device and store it offline.
  - Follow safe practices when browsing the Internet, including Good Security Habits.
- **Employ security tools** that provide link filtering, Domain Name System (DNS) blocking/filtering, malware detection, and intrusion detection and prevention.
- **Adopt Zero Trust/least privilege**: Restrict users' ability to install and run software, and apply the principle of least privilege to all systems and services.
- **Update software and operating systems** with the latest patches. Outdated applications and operating systems are the target of most attacks.

1. 2020 Webroot Quarterly Threat Report, February 2020
2. IDAgent.com, July 2020
3. TechradarPro.com, May 2019

The Unisys Stealth® software suite protects the critical with identity-driven micro-segmentation techniques, robust encryption, and dynamic isolation. Trusted by organizations worldwide to secure sensitive systems, Stealth™ prevents and minimizes the impact of cyberattacks across networks, environments, and devices from inside and outside the perimeter.

- **Use application whitelisting** to allow only approved programs to run on a network.
- **Enable strong spam filters** to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- **Scan all incoming and outgoing emails** to detect threats and filter executable files from reaching end users.
- **Configure firewalls to block access** to known malicious IP addresses.
- **Arrange for rapid access to new servers or endpoints** in case the ransomware infects the BIOS of your current systems.

Also, consider **anti-encryption technologies** such as Endpoint Detection and Response (EDR) solutions that restrict a system's ability to encrypt locally. Utilizing such technologies will often prevent ransomware's signature encryption chaos. It is acknowledged, however, that EDR solutions can be expensive as well as difficult to configure and manage.

2. Minimize the Impact

In addition to defending systems against attack, take action to minimize the impact of a breach. This is critical, since all systems are capable of being breached if an attacker or bad actor has sufficient time and resources to carry out their objective.

First, **back up and restore files structure**. Conduct periodic (at least annual) exercises to recover and restore files.

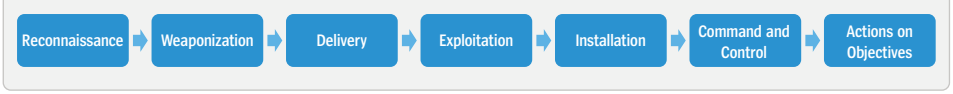
Second, put in place a solid **Incident Response (IR) program**, and practice it periodically. Planning ahead builds confidence in your IR capability. Review your IR policies, engage in tabletop exercises, and use operational benchmarking to improve your ability to respond before an incident occurs.

Third, implement **micro-segmentation**. Micro-segmentation partitions networks to prevent attacks from spreading via east-west proliferation. If a system is compromised, the infection cannot spread out of the micro-segment it is on, significantly reducing the damage that can be done to your environment.

Fourth, enable **dynamic isolation**. Dynamic isolation allows you to isolate a device or user at the first sign of compromise, stopping attacks in their tracks. For example, if a system begins scanning an environment, the device can be isolated immediately until the situation can be reviewed. Too many organizations ignore this concept when, in reality, it is possible to prevent mass infection by focusing here.

3. Break the Cyber Kill Chain®

To better understand how to protect your enterprise, consider the Cyber Kill Chain®, originally defined by Lockheed Martin. The Cyber Kill Chain® outlines the steps which a threat actor will take to infect a host and spread malware. Here is a brief recap of the process, along with the tools that can be used to thwart an attacker.



Once the user downloads the malicious file and it is executed, the attacker gains control and takes action to achieve their objectives.

Reconnaissance and Weaponization

The attacker usually starts with reconnaissance. They choose their target and collect publicly available information about it. Based on that information, they select the appropriate vehicle to weaponize with malware.

Reconnaissance can also involve an attacker with access to the environment who is running network scanning and other tools to build an asset/vulnerability inventory. With this inventory, it is much easier to launch a pre-configured exploit against known vulnerabilities.

Delivery

The attacker then decides how to distribute the payload. This is often done through phishing, spear phishing, or whaling emails because people are very susceptible to deception and easy to target. The attacker will send a user a cleverly-crafted email with a link to click or a weaponized document to open (e.g., PDF files, Word documents, Excel workbooks, etc.).

Ransomware can also be delivered directly through infected websites. In such a case, the site itself has malicious code embedded in it, or contains weaponized files to be downloaded.

Break the Cyber Kill Chain® here through:

- Link filtering
- DNS blocking/filtering
- Malware detection
- Monitoring malicious behavior to block known malicious email addresses

Exploitation and Installation

Next attackers penetrate the target, but they don't necessarily release the malware promptly. Instead, they dwell there to maximize their impact, roaming the network undetected, corrupting additional devices and discovering and perhaps exfiltrating data. According to one report, attackers have increased their dwell time in victim environments to 60 days before delivering their ransomware payloads. Once they deliver it, they wait for the user or employee to click on the link, visit the site, or open a weaponized document. When that happens, the malware is installed and executed.

Break the Cyber Kill Chain® here by:

- Educating users about phishing and other forms of social engineering
- Providing a simple and effective process for employees to report suspicious emails
- Utilizing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), including Endpoint Detection and Response (EDR) and anti-ransomware solutions

Command and Control and Action on Objectives

Once the user downloads the malicious file and it is executed, the attacker gains control and takes action to achieve their objectives.

Break the Cyber Kill Chain® here by isolating the machine through:

- Sandboxing
- Network-based isolation/micro-segmentation
- Host-based isolation, e.g., EDR
- Physically unplugging affected devices

4. Respond to an Attack

Hackers are increasingly sophisticated, so it is likely that a ransomware attack will breach your system(s) at some point. When that occurs, take the following four steps to minimize the impact and recover your data.

First, Execute Your Ransomware Plan

Having a Ransomware Plan will expedite your recovery from an attack, minimizing downtime. This plan should determine **in advance** your company's policy on paying a ransom. Experts recommend ***not*** paying, for multiple reasons:

The easiest and safest method of recovery is to wipe the infected systems and rebuild them from a known good backup.

- There is no guarantee that you will actually get your data back after paying. You might pay, only to have the attacker demand more money or to return later to with another attack.
- You might find yourself in violation of recent warning from the U.S. Treasury's Organization of Foreign Assets Control, and subject to severe penalties.
- Paying rewards bad actors and encourages more ransomware payment demands, exacerbating the already-massive risk.

Second, Identify the Nature of the Attack

This is a step that many overlook. It is highly recommended that you utilize a platform that can identify the nature of the attack. By spending a few minutes figuring out what has happened, you can learn important information such as what variant of ransomware infected your network, what files it normally encrypts, and what options you have for decryption. You may also learn ways to defeat the ransomware without paying or restoring your systems from scratch.

Third, Isolate Infected Devices

Ensure that the infected devices are removed from the network. If they have a physical network connection, unplug it. If they are on a wireless network, turn off the wireless hub/router. Unplug any directly-attached storage to try to save the data on those devices. The goal is to prevent the infection from spreading and impacting more of your environment. Use software-defined micro-segmentation to segment the network into much smaller groups of workloads, managed with identity-driven security policies, to respond rapidly and prevent spreading.

Fourth, Recover and Restore

In general, there are three options to recover from a ransomware attack:

- **Remove the Ransomware**: Depending on the type of ransomware involved, you might be able to remove it without requiring a full rebuild. This process, however, can be very time-consuming and is therefore not a preferred option. Immediately ensure that any users impacted update their credentials.

Mathew Newfield
Mathew Newfield is the Corporate Chief Information Security Officer at Unisys, responsible for design, development and implementation of the company's information security and risk programs across all regions and functions. Before joining Unisys, he was the Director of Global Managed Security Services for IBM responsible for delivery services in 133 countries and a staff of 1,500 security professionals. Prior to IBM, Mathew held senior security leadership roles at Cybertrust, RSA and DDC Advocacy. A published author, speaker and SANS Institute instructor, Mathew holds a Bachelor of Science degree in Industrial and Organizational Psychology from George Mason University.

He can be reached at Mathew.Newfield@unisys.com or connect with him at LinkedIn.

Prof. Sally Eaves
Dr. Sally Eaves is Senior Policy Advisor for Global Foundation for Cyber Studies and Research Forbes, CTO and AI/Cyber/Cloud/Blockchain and CSR Strategic Adviser, Professor of Emergent Technology, International Speaker and Author, Senior Policy Advisor, Global Foundation for Cyber Studies & Research, United Nations Advanced Technology and Social Impact Leadership Founder and CEO of Aspirational Futures.

She can be reached at Social@sallyeaves.com or connect with her at LinkedIn.

- **Wipe and Rebuild**: The easiest and safest method of recovery is to wipe the infected systems and rebuild them from a known good backup. Once rebuilt, you need to ensure that no traces remain of the ransomware that led to the encryption. Some ransomware is capable of impacting the machine level, which is why identification is critical in determining if you can rebuild or need to replace the hardware. Determine if the ransomware has affected the BIOS on your current systems; if so, deploy your plan for accessing new servers or endpoints.
- **Restore**: Once ransomware has been remediated, restore last known good backup files.

5. Lessons Learned

Once you recover from the ransomware, review any gaps or inefficiencies encountered and develop a plan to ameliorate them. Also, update your ransomware plan accordingly.

Once your environment is rebuilt, the real work begins. A full environmental review must take place to determine exactly how the infection began and what steps you need to take to reduce the potential of another breach.

Summary

By putting in place sound preventative measures, understanding the Cyber Kill Chain®, and knowing how to respond to a breach, you can lower your risk of infection and reduce the impact of a breach. Your goal is to be prepared with a plan if a breach occurs so it does not become a newsworthy and costly incidence by fending off the majority of attacks and dealing swiftly and smoothly with those that do manage to penetrate your defenses, you will help keep your business on track, your customers and employees protected, and your reputation intact.

About Unisys

Unisys is a global IT services company that delivers successful outcomes for the most demanding businesses and governments. Unisys offerings include digital workplace services, cloud and infrastructure services and software operating environments for high-intensity enterprise computing. Unisys integrates security into all of its solutions. For more information on how Unisys delivers for its clients across the government, financial services and commercial markets, visit www.unisys.com.

To minimize impact to your business operations from a ransomware attack, learn more about dynamic isolation at www.stealthsecurity.unisys.com/use-case-dynamic-isolation/.

For more information visit www.unisys.com

02/21 21-0078