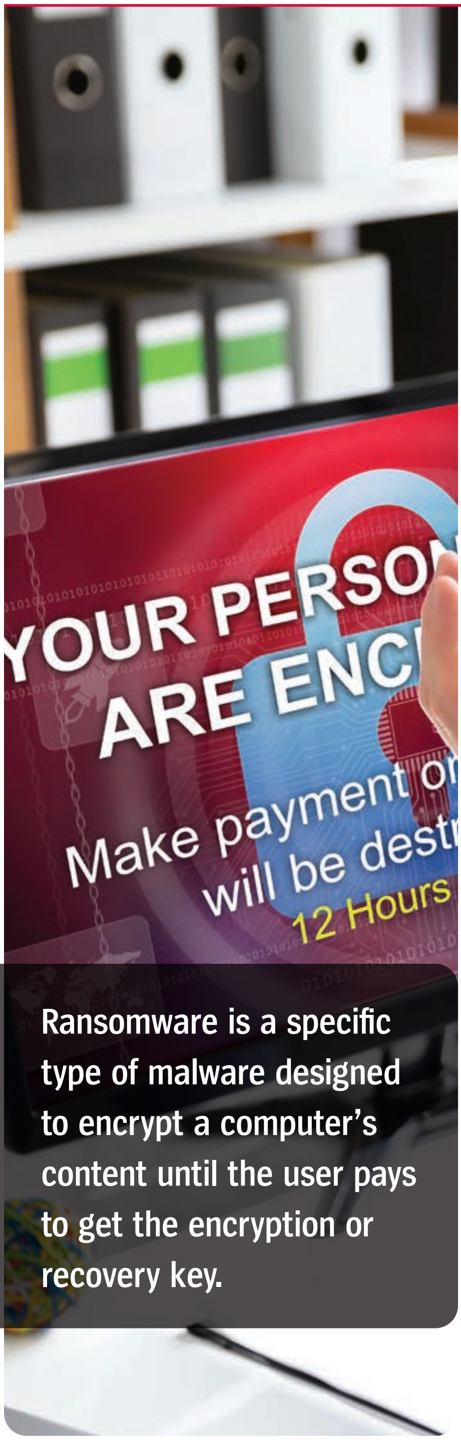
UNISYS | Securing Your Tomorrow®

# 4 Ways to Deliver a Deadly Counterpunch to Ransomware Attacks.

By JP Cavanna



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

With phishing sites growing by 640% in 2019[1] and 65% of ransomware attacks delivered via phishing[2], the threat of ransomware hangs over every IT professional. Ransomware is a specific type of malware designed to encrypt a computer's content until the user pays to get the encryption or 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. To protect your 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 consider these preventative steps.

## 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:

- **Follow best practices** such as strong patching policies, regular system backups, Multifactor Authentication (MFA), and restrictions of local administrator rights and privileges.
- **Conduct awareness programs** to educate users about phishing and other forms of social engineering.
- **Employ security tools** that provide link filtering, Domain Name System (DNS) blocking/filtering, virus detection, and intrusion detection and prevention.
- **Adopt Zero Trust/least privilege**: Restrict users' persmissions to install and run software aplications, 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.
- **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.

[1] 2020 Webroot Quarterly Threat Report, February 2020

[2] IDAgent.com, July 2020

*The attacker usually starts with reconnaissance. This is where they choose their target and collect publicly available information about that target.*

- **Encourage and train users** to:
  - Never click on links or open attachments in unsolicited emails.
  - Backup data on a regular basis. Keep it on a separate device and store it offline.
  - Follow safe practices when browsing the Internet, including there Good Security Habits.

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.

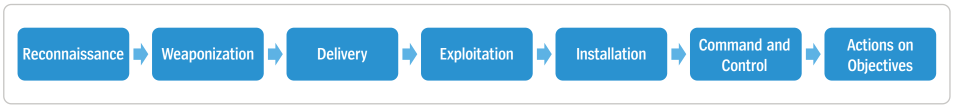
First, put in place a solid **Incident Response (IR) program**. Planning ahead builds confidence in your IR capability. To that end, review your IR policies, engage in tabletop exercises, and use operational benchmarking to improve your ability to respond before an incident occurs.

Second, 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.

Third, 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.



Reconnaissance → Weaponization → Delivery → Exploitation → Installation → Command and Control → Actions on Objectives

### Reconnaissance and Weaponization

The attacker usually starts with reconnaissance. This is where they choose their target and collect publicly available information about that target. From there, they select the appropriate vehicle to weaponize with malware based on the information they gained while performing reconnaissance.

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

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

### 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
- Virus detection
- Application whitelisting
- Inbound/outbound transport rules to block known malicious email addresses

### Exploitation and Installation

Once the bad actor has delivered the payload, they wait for the user or employee to click on the link, visit the site, or open a weaponized document. When this 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 host-based IDS and IPS
- Employing anti-encryption technologies, such as EDR 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, e.g., Unisys Stealth®
- 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.

*Hackers are increasingly sophisticated, so it is likely that a ransomware attack will breach your system(s).*

### Step 1: Isolation

Before doing anything else, 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. Additionally, unplug any directly-attached storage to try and save the data on those devices. The goal is to prevent the infection from spreading and impacting more of your environment. Using software-defined micro-segmentation can segment the network into much smaller groups of workloads, manged with identity-driven security policies, to prevent spreading and to respond rapidly.

### Step 2: Identify

This is a step that many people overlook. It is highly recommended that you utilize a platform such as Crypto Sheriff to 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 you, 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 system(s) from scratch.

### Step 3: Report

This is another step that many security professionals ignore, whether due to embarrassment or time constraints. However, by reporting the ransomware attack, you potentially help other organizations avoid a similar situation and you provide law enforcement with a better understanding of the attacker. There are many ways to report a ransomware attack. For example, in the United States, you can contact your local FBI office or register a complaint with their Internet Crime Complaint Center website. You can also report attacks on websites such as On Guard Online or SCAMwatch.

### Step 4: Recover

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

- **Pay the ransom**: This is not recommended because there are no guarantees that you will actually get your data back after paying. For example, you might pay the ransom only to be told that the attacker wants even more money before unencrypting the data.
- **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.
- **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. In this regard, a solution like Dell Cyber Recovery Vault with Stealth™ would allow an organization to rebuild quickly.

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.

*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.*

**JP Cavanna**

JP is a passionate cyber security leader with a career that spans 17 years. He has held several director positions building and managing cyber professional services businesses in large UK and global organizations, spanning a diverse range of industry sectors. Consequently, he has deep experience in helping clients to create resilient security environments.

He can be reached at
johnpaul.cavanna@unisys.com
or connect with him at
LinkedIn.

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 not to guarantee that a ransomware attack will never be successful, as that is an impossibility. Rather, your goal is to ensure that if a breach occurs, it does not become a newsworthy event. By fending off the majority of attacks and dealing swiftly and smoothly with the few hackers who get in the door, you will help keep your business on track and on target.

## About Unisys

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most digitally demanding businesses and governments. Unisys offerings include security software and services; digital transformation and workplace services; industry applications and services; and innovative software operating environments for high-intensity enterprise computing. For more information on how Unisys builds better outcomes securely 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