WHITE PAPER

The How to Survive the Ransomware Rampage

RIDGE SECURITY

The How to Survive the Ransomware Rampage

Ransomware is blackmail: an extortion proposition where bad actors seek to monetize hijacked data from an organization's compromised applications and systems. As victimized organizations have become less inclined to pay the ransoms, bad actors have developed new and increasingly threatening approaches to extort large payments. Beyond holding data ransom by encryption, they are combining encryption with other methods to encourage the probability of payments.

It often seems that every other day news breaks from somewhere around the globe about yet another business or government affected by a ransomware attack that resulted in devastating consequences. An attack on the Düsseldorf University Hospital in Germany in September 2020 resulted in loss of life as an emergency patient had to be diverted to another facility and could not be cared for in time. An attack on SMP Health in Illinois in early 2021 has led to the closure of a hospital facility.

While ransomware has maintained prominence as one of the most significant global threats, payouts during recent years have yielded enough damage to solidify its position as a boardroom and government executive risk. Every aspect of the attacks is on the increase.

- The number of victims
- The number of payouts
- The amount of the payout demanded
- The damage to organizations and their supply-chains
- Extortion for stolen data, in addition to the ransom for decrypting data

A BlackFog report states that "In April [2023], we saw continued growth in education, government and healthcare of 19%, 20% and 24% respectively, with the tech sector seeing the biggest growth of 40% this month. Unreported attacks are now 10 times those of reported."

In addition to the financial burdens of payouts, ransomware attacks have widened the scope of inflicted damage to also threaten data privacy, national security, industrial security, food security and healthcare.

Ransomware Trends

Several trends are fueling the rapid rise in both frequency and size of attacks. Threat actors are also adjusting their playbook for higher-impact targets to gain larger and more assured payouts.

Trends Fueling Increased Ransomware Attacks

Several digital business and industry trends have dramatically increased the attack surface of commercial enterprises, public and private organizations, as well as government networks. Other trends have opened up new opportunities.

- **Cloud migration:** Cloud-based technology has rapidly grown over the last several years providing significant cost savings and business agility to all sizes of organizations. Cloud platforms and services afford companies significantly increased flexibility in storage, computing and grow-and-shrink suppleness at pay-as-you-use rates instead of heavy capital infrastructure investment. Increasingly, workloads are hosted in cloud environments.

- **Work-from-Anywhere:** The covid pandemic response caused a momentous and sudden shift to a work-from-anywhere (WFA) professional workforce. Some portion of this shift has proven permanent. Organizational efforts to maintain business continuity during covid lockdowns accelerated cloud migration. Together, the cloud and WFA trends dissolved the traditional physical network perimeter, substituting it with a software-defined perimeter (SDP) that runs along every surface of the network open to Internet access. The industry is struggling with the ever-changing abilities and technologies to properly secure the much larger attack surface of the new soft, and often virtual, perimeter.

- **IoT:** Unmanaged low-cost devices are proliferating in networks to automate, observe, report, measure, monitor and surveil a wide-ranging array of consumer and commercial devices and situations, from manufacturing to farming. IoT devices often use obsolete copies of open-source TCP/IP stacks, lack even rudimentary security capabilities, and offer no methodology for tracking or installing patches for known vulnerabilities.

Other trends more specific to ransomware have also led to a significant increase in the sophistication, impact, and financial efficacy of the attacks.

- **Ransomware-as-a-Service (RaaS):** In the past, attack targets were naturally limited because only a few highly-skilled threat actors had the infrastructure, technical ability and fine-tuned execution methodology to infiltrate the well-secured networks of large organizations and governments.The criminal business model has now matured with highly sophisticated services-for-hire. RaaS is readily available in the cloud, and customizable ransomware kits that can be purchased on the dark web and be deployed with ease. This lowered the bar to entry and enabled a much larger population of threat actors to launch sophisticated attacks. RaaS offers different types of affiliate partner programs, with a full-fledged web portal where affiliates can get updated kits. REvil/Sodinokibi and Netwalker are examples using a RaaS model.

- **Spam, Phishing and RDP:** This continues to be the most successful initial entry-point for malware. Phishing emails, RDP (Remote Desktop Protocol) exploitation, and exploitation of software vulnerabilities remain in the top initial infection vectors for ransomware incidents.

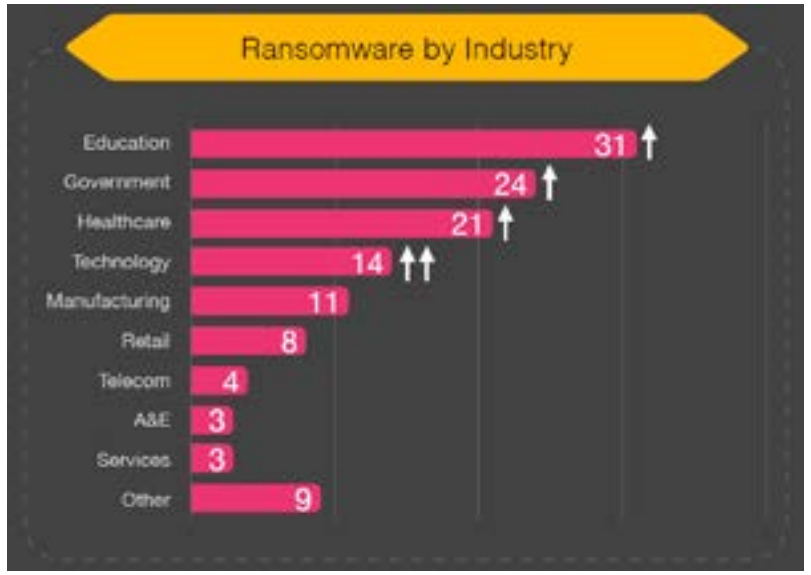
- **Bitcoin Payments:** The growing popularity and availability of crypto-currencies such as bitcoin offer payment methods with no traceability, no option to dispute, and un-cancelable transactions.

- **Increased impact:** Ever-more sophisticated ransomware attacks have shifted from small and medium-sized businesses to target critical government and infrastructure organizations globally, including defense, emergency services, food supply, government facilities, healthcare organizations, financial services, education, research facilities, communication services, and energy sectors. To enlarge the scope and impact of attacks, threat also actors target managed services providers (MSPs), industrial processes and software managing supply chains.

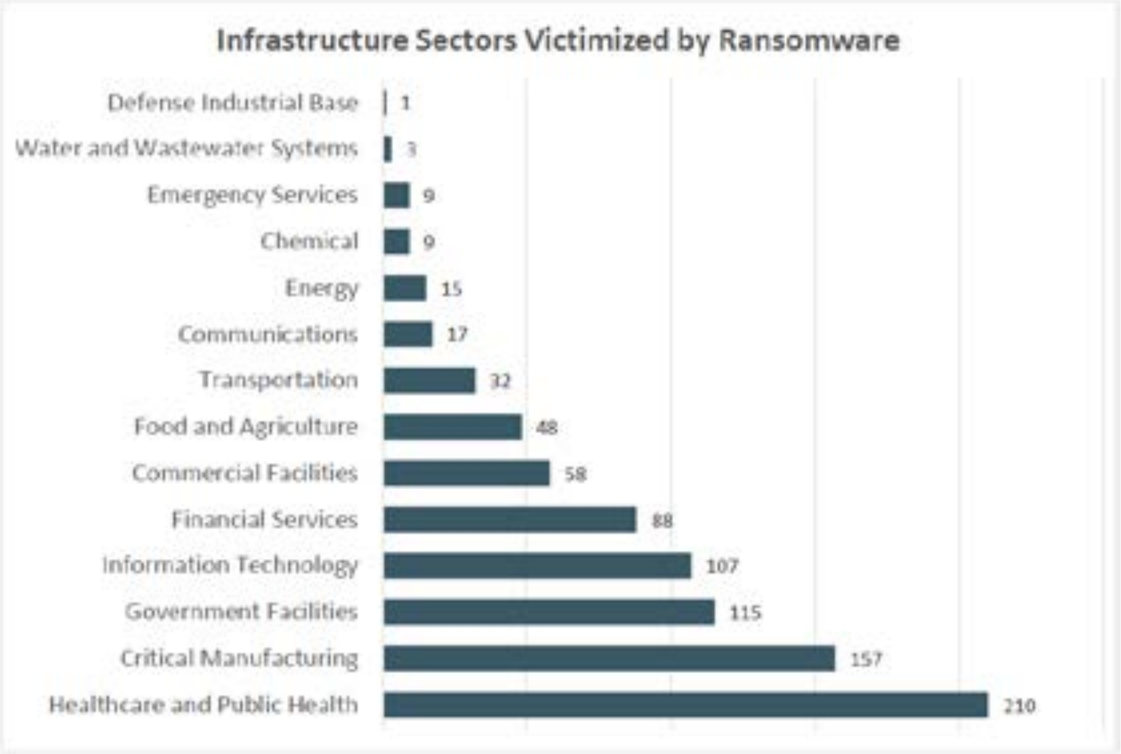
Type of Target Sectors

Ransomware still occasionally targets consumers, but the vast majority of attacks have shifted to focus on corporate, industrial and government targets, especially those with regulatory exposure. The initial asset infiltration is almost as easy and the payout opportunities are enormous. The prospect of regulatory fines and reputation damage resulting from publicly exposed data privacy violations as well as government embarrassment and reputation damage significantly increase the success rate and size of payouts.

In 2023, BlackFog reports the following distribution of industry segments most targeted by ransomware.



The FBI Internet Crime (IC3) Report of 2022 reports the following distribution of infrastructure sectors most targeted by ransomware.



Attack Approaches

Ransomware has seen considerable **growth in virulence**, and—empowered by RaaS—a **larger population of threat actors** who can target a larger number of victims.

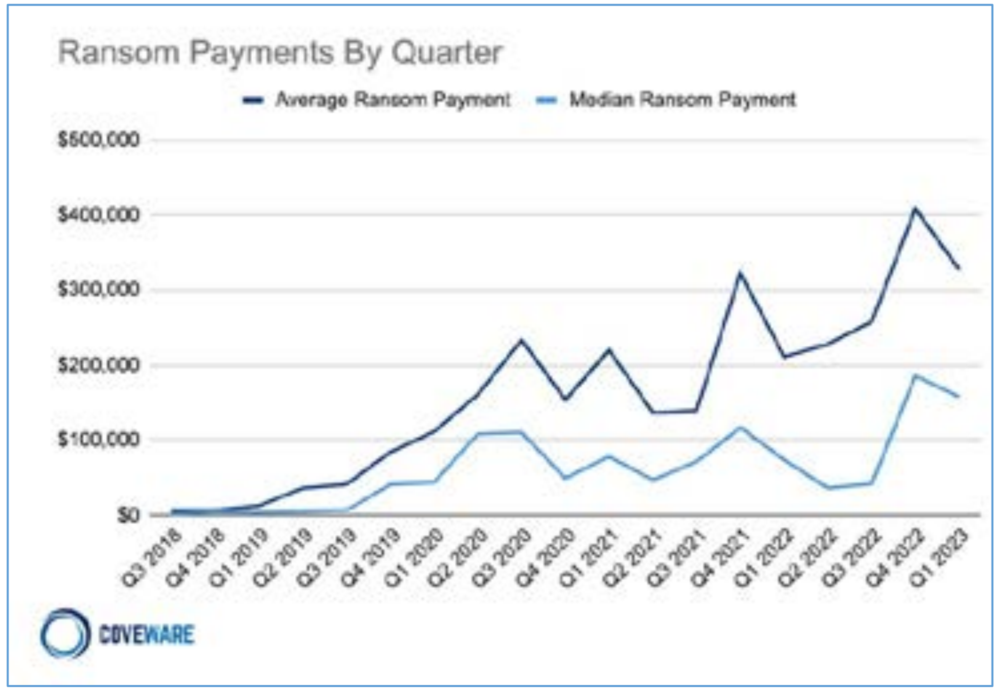
In addition to simply holding an organization's data to ransom by encryption, an increasing number of the more recent attacks **combines encryption with extortion** to boost the probability of a payment. In these combination attacks, the threat actor first gains access to the organization's assets and exfiltrates their data, and only then encrypts it. If the organization refuses a payout for the decryption key, the threat actor exposes the exfiltrated data by making it publicly available, or auctioning it on the dark web, thereby damaging the organization's reputation and financial well-being.

This trend results in ransomware attacks also becoming data breaches. It forces organizations' security management to re-assess risk and incident response, and adjust disaster recovery and business continuity strategies. Ransomware groups continue to leverage this data exfiltration and extortion tactic, though trust that stolen data will be deleted is eroding as defaulting on the promises are becoming more prevalent despite the victim paying the ransom.

Threat actors are also taking advantage of security vulnerabilities exposed by cloud migrations and WFA that often remain unaddressed for a period of time. The proliferation of WFA setups using RDP and other remote access technologies allow threat actors to leverage attack vectors that didn't exist until the last few years.

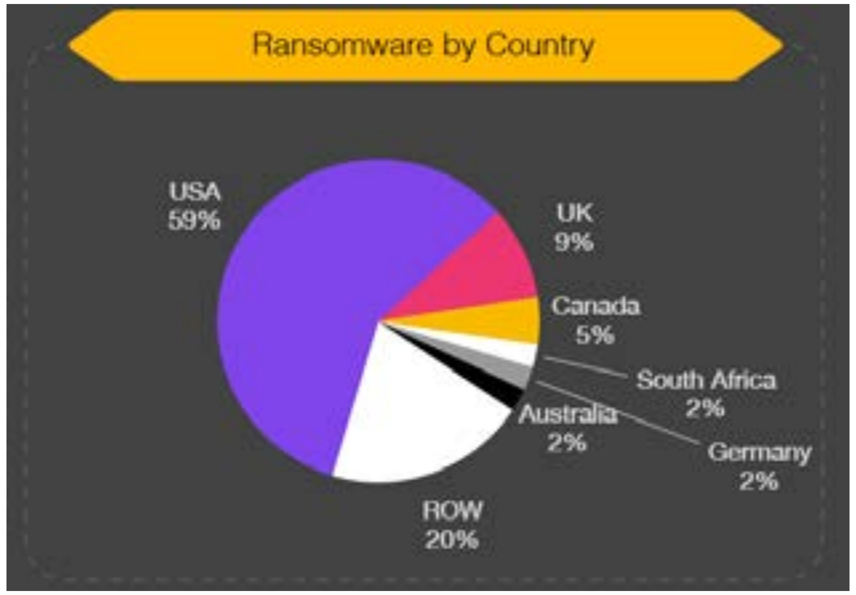
Payouts

In recent years, reporting by Coveware shows that the **average ransom payout** fluctuates, but the trend is inexorably upwards. The increase is partially attributed to attackers targeting larger companies and institutions



Geographic Distribution

Ransomware attacks primarily target **North-America and Europe**, although no country or organization in the world is exempt. BlackFog reports the following country distribution:



Operating Systems

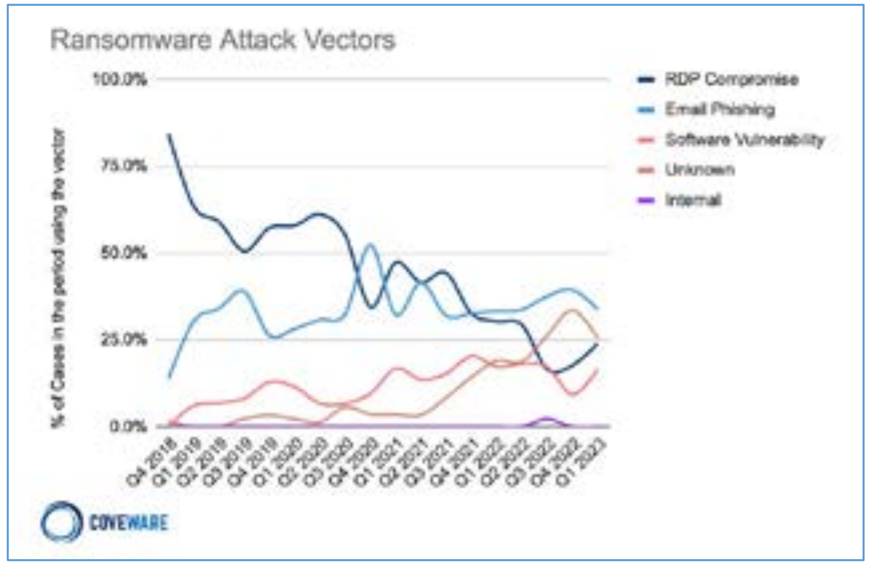
Traditionally, threat actors have targeted Windows systems as the largest **operating system installed** base, but MacOS and Linux platforms are increasingly targeted also.

Attack Vectors

The evolving criminal business model often complicates attribution because of the complex networks of developers, affiliates, and freelancers involved. It is frequently difficult to positively determine the actors behind a ransomware incident.
Most ransomware attacks pivot on a small number of common infection vectors.

- **Remote Desktop Protocol (RDP):** Network intrusion through unsecured ports and services.
- **Phishing:** Malicious email attachments, also termed “malspam”.
- **Software and Network Vulnerabilities:** Worms and other ransomware forms that exploit network vulnerabilities.
- **Dual Malware:** Additional malware dropped in via previous malware infections (for example, a TrickBot infection leading to a subsequent Ryuk infection).

Coveware reports the following distribution of attack vectors.

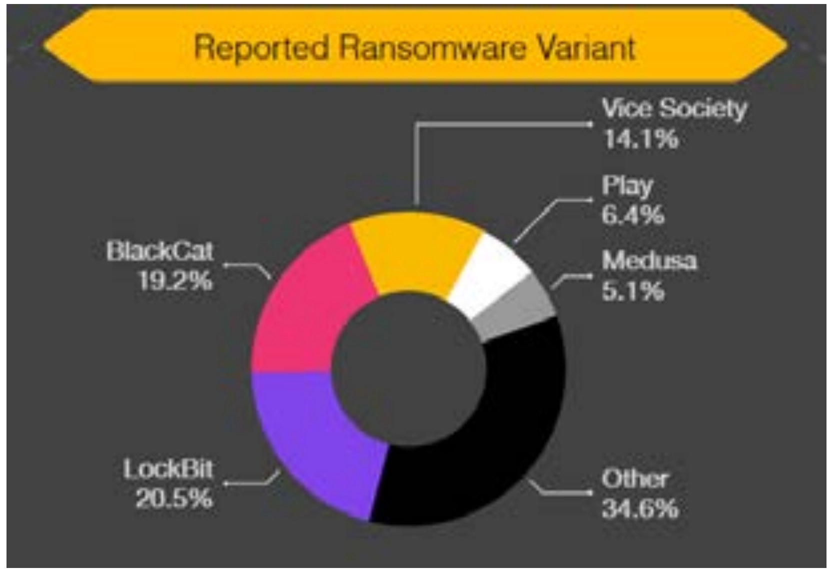


Ransomware Tradecraft

Improvements and changes to ransomware tradecraft observed in the industry include:

- More stealth, less noise: ransomware engagements are fast, but they are loud
- Tooling improvement: less reliance on standard penetration testing tools, and using more bespoke malware
- Faster time to attain domain admin credentials
- Improved ransomware deployment methods
- Increased effectiveness to delete backups

A BlackFog report summarizes the distribution of ransomware variants observed as follows:



Recommended Mitigation Actions

Even the simplest attack can cause an organization significant time and money. Sophisticated attacks, and combined extortion-encryption attacks, can cause a crippling blow or entirely destroy a company. Immediate actions you can take to protect against ransomware are listed below. RidgeBot can help you determine which patches and upgrades are critical, and which ones are lower priority because they do not pose a realistic risk of exploitation.

- Ensure all operating systems have up-to-date patches, and install antivirus software everywhere.
- Raise awareness with employee education about social engineering, phishing strategies and highlight the risks of suspicious links and attachments.
- If you use RDP, secure and monitor it.
- Establish and maintain offline backups, and regularly test these to ensure systems can be rebuilt successfully.

Additional general recommendations to minimize damage from a ransomware attack include:

- Establish a strategy to prevent unauthorized data theft—especially where large amounts of data are stored or uploaded to cloud platforms.
- Institute user behavior analytics to monitor and identify potential security incidents.
- Use multifactor authentication (MFA) on all remote access points.
- Deploy regular or continuous penetration testing to identify weak points, weak credentials and frequently exploited vulnerabilities.
- Deploy Secure Access Service Edge (SASE) technologies to lock down the soft perimeter (SDP) around cloud assets, DIA at office locations, and WFA employee access.
- Specific actions to mitigate TCP/IP protocol stack vulnerabilities (for normal enterprise assets as well as IoT): disable IPv6 when/where not needed; rely on internal DNS servers for critical devices; monitor your network for anomalous packets and behavior; segment your network to prevent lateral movement of malware.
- Be wary of publicly exposed services such as Remote Desktop (RDP, port 3389), VPN, Virtual Network Computing (VNC), FTP, and Server Message Block (port 445).
- Don't install software or give it admin privileges unless you know exactly what it does.

Techniques and Operating Modes

Common tactics and techniques used by ransomware authors and operators fall into several categories.

- **Opportunistic:** The operating model of opportunistic actors is self-propagating ransomware such as WannaCry. The threat actors initiate the malware—often using easily accessed entry points such as exploit kits, backdoors, open ports, unsecured VPNs, operating systems and applications lacking patches—but after that it is up to user actions to propagate it and the threat actors don't know where it is going, where it is going to move to, what target organization may fall victim, or what domains or networks it may access.

  Sometimes called spray-and-pray, these are high-volume, less sophisticated attacks and is an operating method that has recently been on the decline.

- **Targeted:** This is a lower volume, more sophisticated, strategic technique that results in higher average payouts. Threat actors use a specific campaign to target a particular organization.

  They gain access to the network through phishing emails, social engineering, operating system or open port vulnerabilities, and then look around the network before unleashing their ransom demands. There are two operating modes in this "targeted" technique:

- **Partnership Model:** Professional "threat authors" create the ransomware, then provide affiliates (by subscription, or percentage of the ransom) with a platform where they can access tools and instructions to execute attacks. This model offers a low barrier to entry for highly sophisticated attacks.

  Another mode of operation in this model is where the "threat authors" create the ransomware and also perpetrate the initial compromise of the targeted organization, and then sell access to affiliates to execute the attack.

- **Self-managed Model:** In this mode of operation the threat actors execute the initial compromise phase themselves, gain access to the system and the environment, then move around before executing the ransom demands.

Harden Your Assets Against Ransomware with Ridgebot

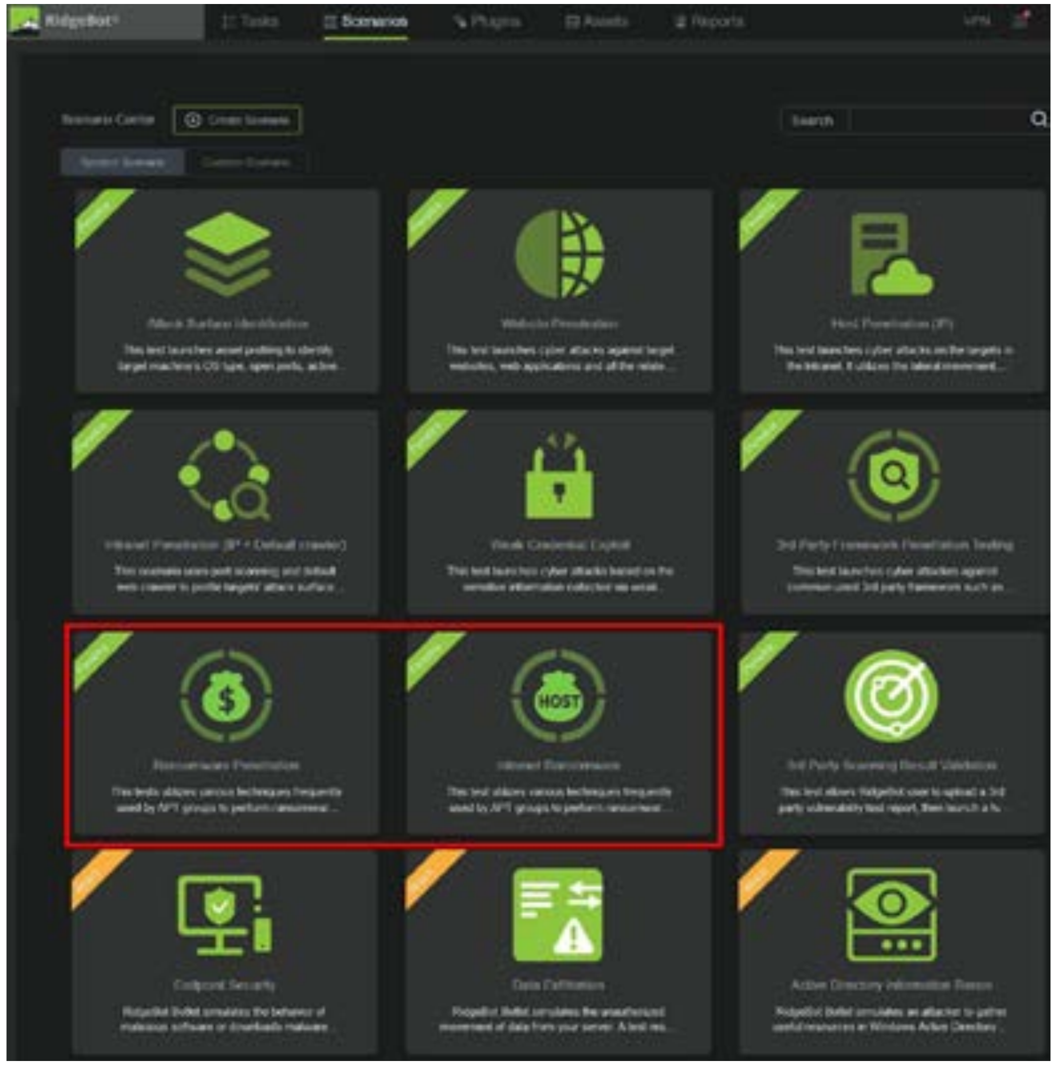
RidgeBot auto-discovers your assets, scans them, and then proceeds to exploit the vulnerabilities found by attacking your assets just as a hacker would. In its report, RidgeBot alerts you to the dangerous, successfully exploited vulnerabilities and also shows you the exact attack path that allowed the asset to be compromised. With this detailed and accurate information, you can quickly and proactively close all the high-priority vulnerabilities in your network and other assets.

Ransomware Protection

RidgeBot includes templates specifically focused on combating ransomware attacks. These templates allow you to easily:

- Scan for more than 280 high-profile ransomware entry point vulnerabilities
- Launch attacks to exploit these vulnerabilities
- Get detailed reports on exactly how successful exploitations were achieved

Additional ransomware attack definitions are regularly added to RidgeBot, so you can boost your security arsenal by downloading periodic RidgeBot updates.



Running the RidgeBot ransomware templates allows you to quickly and easily launch an asset scan to detect ransomware related vulnerabilities that may be present in your assets. As an integral part of the scan, RidgeBot also launches attacks to prove that the vulnerabilities found are indeed exploitable in your current environment. You can run these penetration tests and attacks on demand or on a regular schedule.

As with other vulnerability tools and tests, it is recommended that you re-execute a ransomware template scan-and-exploit run whenever there is any change in your assets, such as

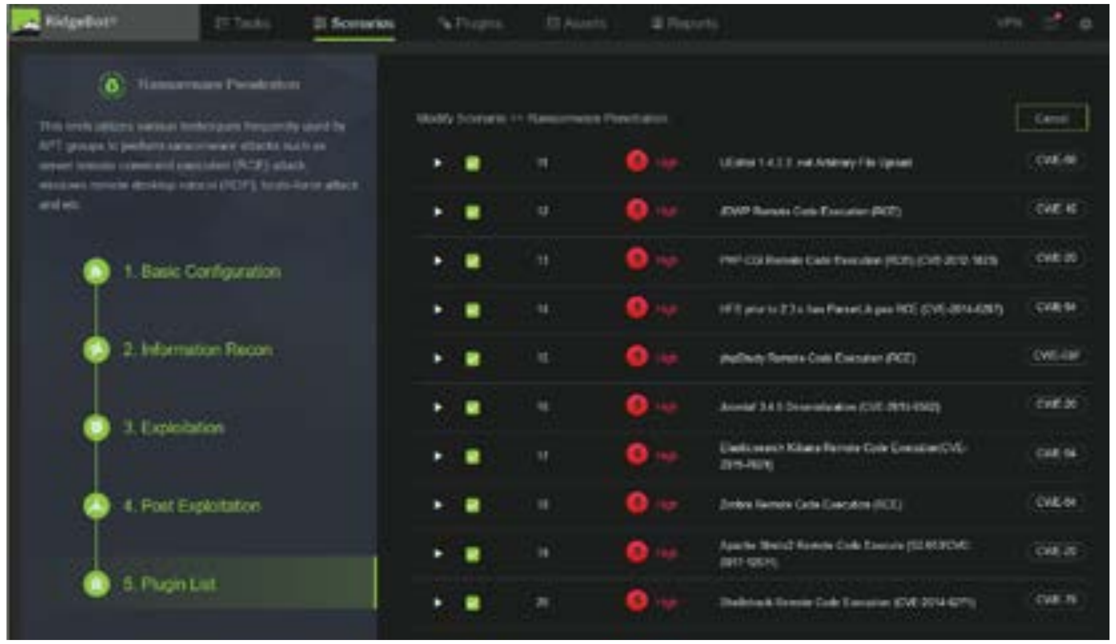
- Adding a new server or network device
- Upgrading software or firmware
- Installing patches
- Change web server scripts or information
- Any other software or hardware change that may result in deploying a new vulnerability in your network. You should be particularly cognizant of IoT devices that may be connected or inserted into your network.

Approach

The RidgeBot ransomware templates include scanning and exploitation for the following classes of vulnerabilities:

- Remote Code/Command Execution (RCE)
- Weak Password and Credential Stuffing (for example, SSH, Redis, and SQL Server)
- Server Message Block (SMB)
- WebLogic and Other File Uploads

RidgeBot scanning and exploitation cover technical vulnerabilities such as weak credentials, open ports, file uploads, WebLogic and Struts2 web application vulnerabilities. Use RidgeBot to locate the vulnerabilities in your network to avoid ransomware intrusions before they happen. Once an intrusion has taken place via social engineering or phishing, or when data has already been encrypted and exfiltrated by a ransomware attack, there isn't much that can help alleviate the situation.

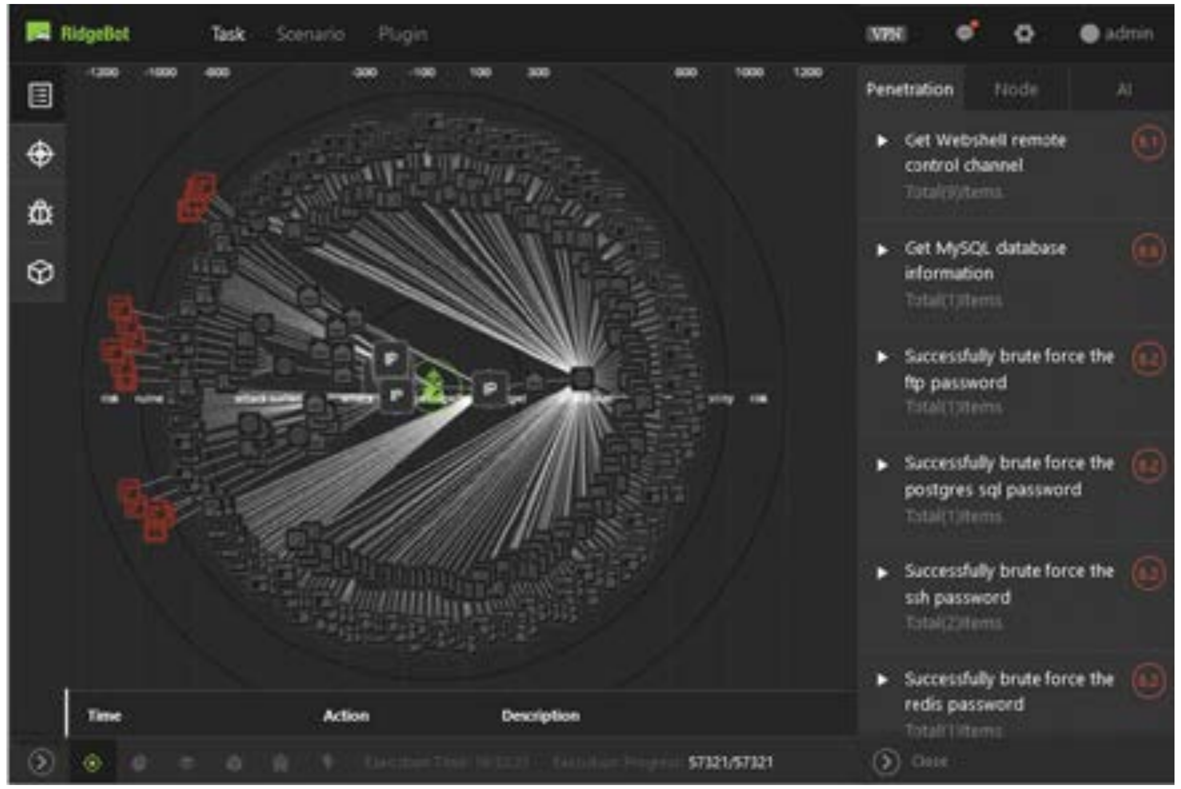


If you consider your organization to be a possible or likely "target organization" for threat actors, then use the RidgeBot scanning and exploitation capabilities to protect yourself against the initial compromise stage of a planned attack. Once a threat actor has entered your network and established a foothold, you additional tools are required to detect and correct the intrusion.

The goal of traditional security scanning software is simply to find as many vulnerabilities as possible. Yet, industry statistics reveal that only ~3% of all vulnerabilities are exploitable, leaving the majority harmless in a typical environment. RidgeBot's scanning and exploitation capabilities help you sift through all the vulnerabilities not only to find them, but—more importantly—to distil out the critical ones that are exploitable in your environment and therefor pose a severe threat to your operations. RidgeBot helps you to not be consumed and distracted by false positives, and patching or upgrading software that pose no realistic threat to you.

Combating Ransomware Attacks with RidgeBot

RidgeBot develops a network structure of discovered assets and shows a list of targets (red boxes on the graphic), and exploits and vulnerabilities (listed on the right side of the screen), that were successfully penetrated. Highlighting any one of these penetrations reveals the exact attack path that RidgeBot followed to compromise that target. This provides you with clear and accurate information on which devices in your environment require what types of fixes or updates to be properly secured against ransomware attacks.



- Get Webshell remote control channel
  Total(9)items
- Get MySQL database information
  Total(1)items
- Successfully brute force the ftp password
  Total(1)items
- Successfully brute force the postgres sql password
  Total(1)items
- Successfully brute force the ssh password
  Total(2)items
- Successfully brute force the redis password
  Total(1)items

Execution Progress: 57321/57321

The sections below provide details and examples of a number of high-profile, exploitable vulnerabilities that may exist in your environment. RidgeBot can protect you against these vulnerabilities and more.

The U.S government agency National Institute of Standards and Technology (NIST) maintains a searchable National Vulnerability Database (NVD) where additional details of all vulnerabilities with allocated CVE numbers can be researched.

Missing Authentication: F5 BIG-IP

In May 2023 CISA (the US Federal Government's Cybersecurity and Infrastructure Security Agency) and the Multi-State Information Sharing & Analysis Center (MS-ISAC) released a joint Cybersecurity Advisory in response to the active exploitation of CVE-2022-1388.

This vulnerability—found in F5 Networks' BIG-IP Application Services software—allows unauthenticated actors to gain control of the system through the management port or self-IP addresses, which in turn allows the attacker to remotely execute malicious code. This exploit uses two techniques: an "admin:" empty token bypasses authentication, and "abusing HTTP hop-by-hop request header" which manipulates the header to enable a remote code execution (RCE) attack.

Deploying automated RidgeBot penetration testing within your network removes these types of CVE risks. RidgeBot's continuous automated pen testing discovers and protects against new and unknown CVEs such as CVE-2022-1388.

RCE: EternalBlue

The massive worldwide ransomware attacks of 2017 made headlines around the globe, paralyzed businesses for several days, and cost several multi-national organizations millions of dollars in damage, repair and recovery. The WannaCry ransomware that hit in May 2017 used the EternalBlue vulnerability to exploit unpatched Windows computers. This was followed in June 2017 by the NotPetya ransomware attack that exploited the same vulnerability.

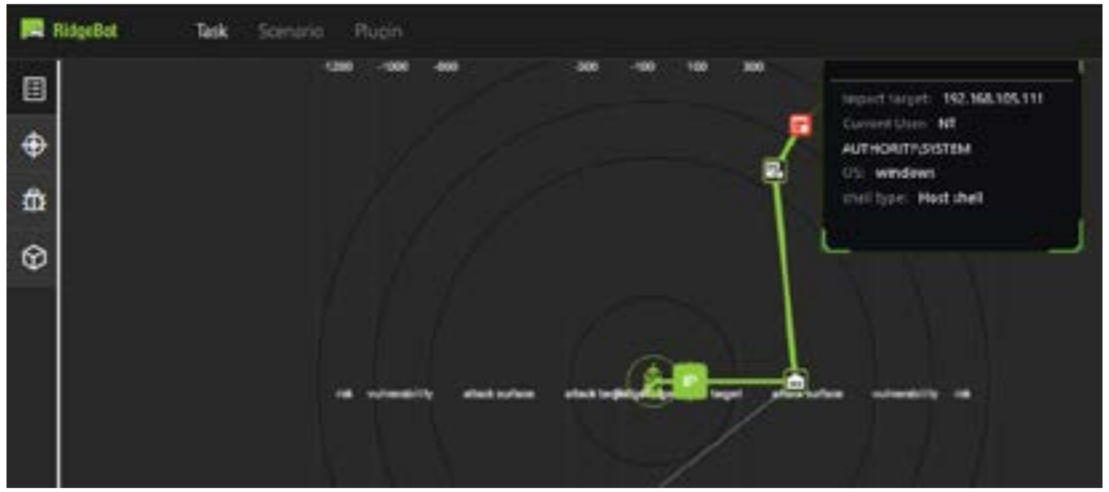
In March 2017, Microsoft issued security bulletin MS17-010 detailing the EternalBlue security flaw and announced Windows patches for all supported versions active at that time. EternalBlue is also covered by CVE-2017-0143-to-CVE-2017-0148.

EternalBlue is an exploit allowing threat actors to gain access to a Windows asset, control the shell, and remotely execute arbitrary code by sending specially crafted packets to a server using Microsoft Server Message Block 1.0 (SMBv1). SMB is a network file sharing protocol to allow access to files on a remote server.

This vulnerability enables threat actors to inject malware that then self-propagates to infect the entire network and all devices connected to it, dropping the crypto-ransomware payload everywhere as it spreads. The self-propagate ability has made EternalBlue a popular exploit for various other malware such as Trickbot (a modular banking trojan), as well as CoinMiner and WannaMine where crypto-miners exploit EternalBlue to gain access to computing resources to mine crypto-currencies.

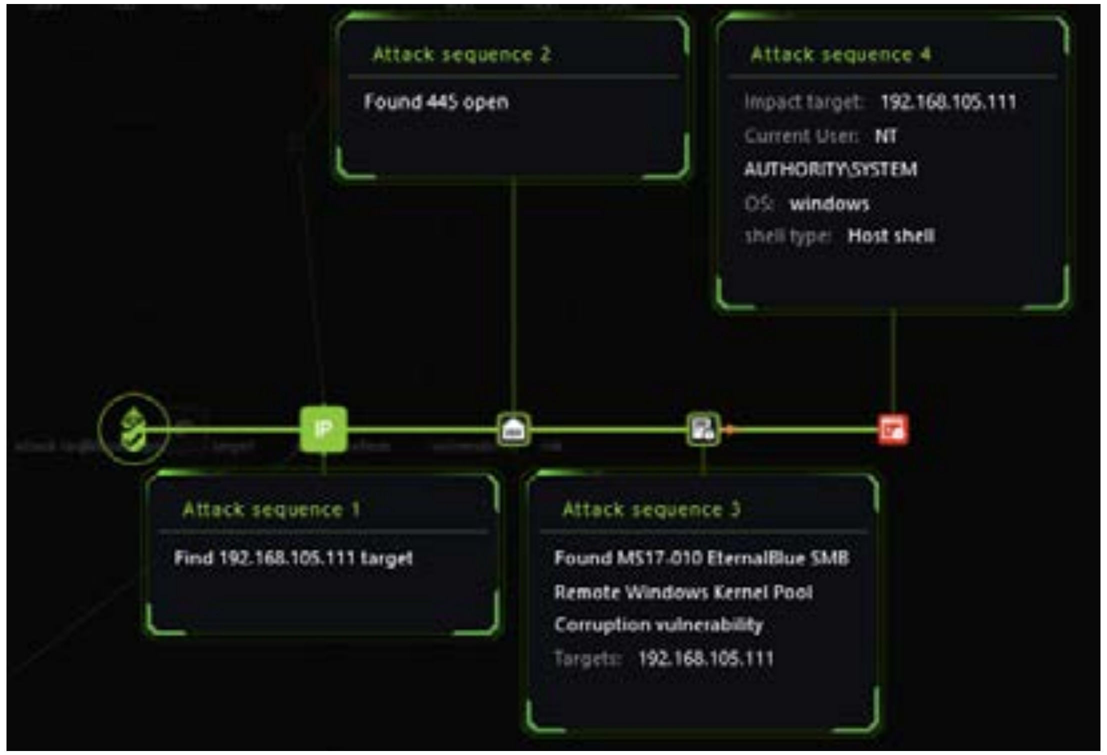
The EternalBlue vulnerability and Windows patches to counteract it were already announced years ago in March 2017. Yet, security company Avast estimates that as of June 2020, they are still blocking around 20 million EternalBlue attack attempts every month.

RidgeBot can scan your network, devices and servers to detect any latent unpatched EternalBlue vulnerabilities in your environment. RidgeBot further launches an attack against the target device by exploiting the EternalBule vulnerability found. In the sample Ridgebot attack against IP 192.168.105.111 shown below, an EternalBlue vulnerability was successfully penetrated (red box at the outer edge).



Impact target: 192.168.105.111
Current User: NT AUTHORITY\SYSTEM
OS: windows
shell type: Host shell

Drilling down on the exploit-path (green boxes) to the compromised target machine (red box), discloses the attack path the threat actor exploited to reach the target.



Attack sequence 2
Found 445 open

Attack sequence 4
Impact target: 192.168.105.111
Current User: NT AUTHORITY\SYSTEM
OS: windows
shell type: Host shell

Attack sequence 1
Find 192.168.105.111 target

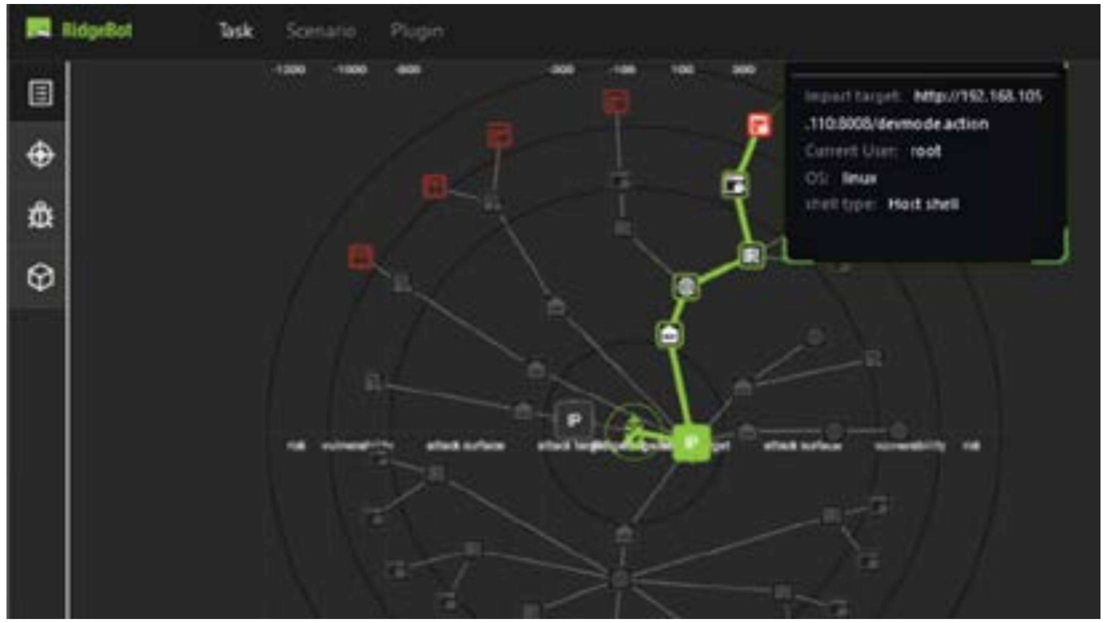
Attack sequence 3
Found MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption vulnerability
Targets: 192.168.105.111

For EternalBlue exploits, RidgeBot can control the host shell of the compromised device. A successful RidgeBot exploit of an EternalBlue vulnerability is given in the Risk Table, showing that the host target was entered and that RidgeBot could issue commands from the shell.

RCE: Struts2

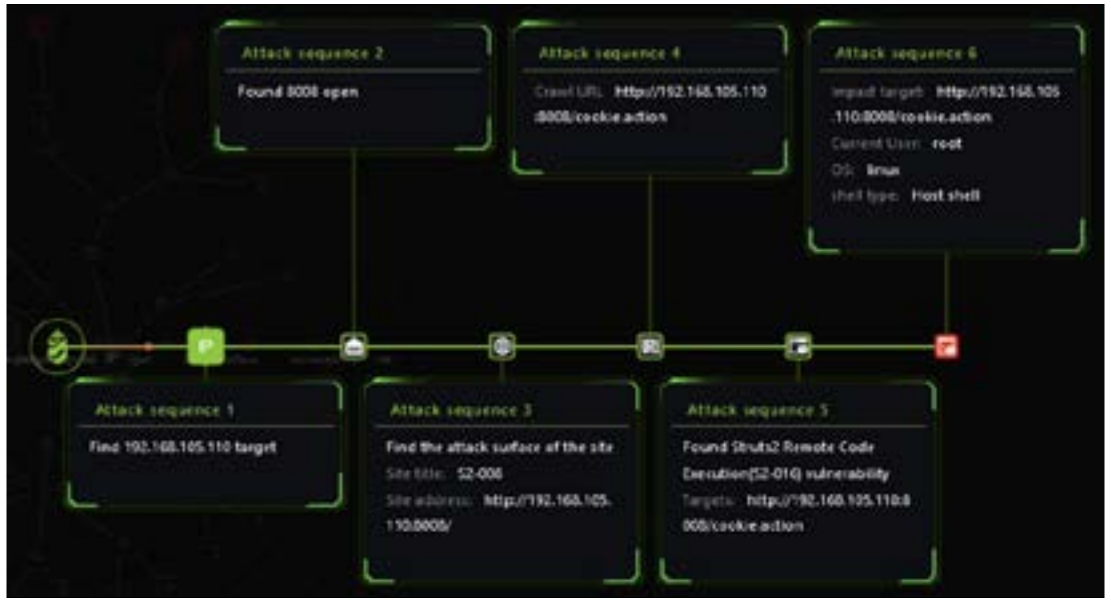
Apache Struts2 is a free, open-source web application (Model-View-Controller, or MVC) framework for developing cross-platform Java web applications. It has an extensible architecture using the Java Servlet API and REST, AJAX and JSON plugins to enable easy software development.
A series of remote code execution vulnerabilities exists in the Struts2 code and plugins, including Apache security bulletins S2-008 (CVE-2012-0391), S2-016, S2-019 (CVE-2013-4316), S2-032, S2-037, S2-045, S2-048, S2-052, S2-057, and S2-059. You can review the details of all Apache Struts2 security bulletins here.

RidgeBot can scan your network, devices and servers to detect any of the above Struts2 vulnerabilities in your environment. RidgeBot further launches an attack against the target device by exploiting the Struts2 vulnerability found. In the sample Ridgebot attack against IP 192.168.105.110 shown below, a Struts2 vulnerability was successfully penetrated (red box at the outer edge).



Impact target: http://192.168.105.110:8008/devmode.action
Current User: root
OS: linux
shell type: Host shell

Drilling down on the exploit-path (green boxes) to the compromised target machine (red box), discloses the attack path the threat actor exploited to reach the target.



Attack sequence 2
Found 8008 open

Attack sequence 4
Crawl URL: http://192.168.105.110:8008/cookie.action

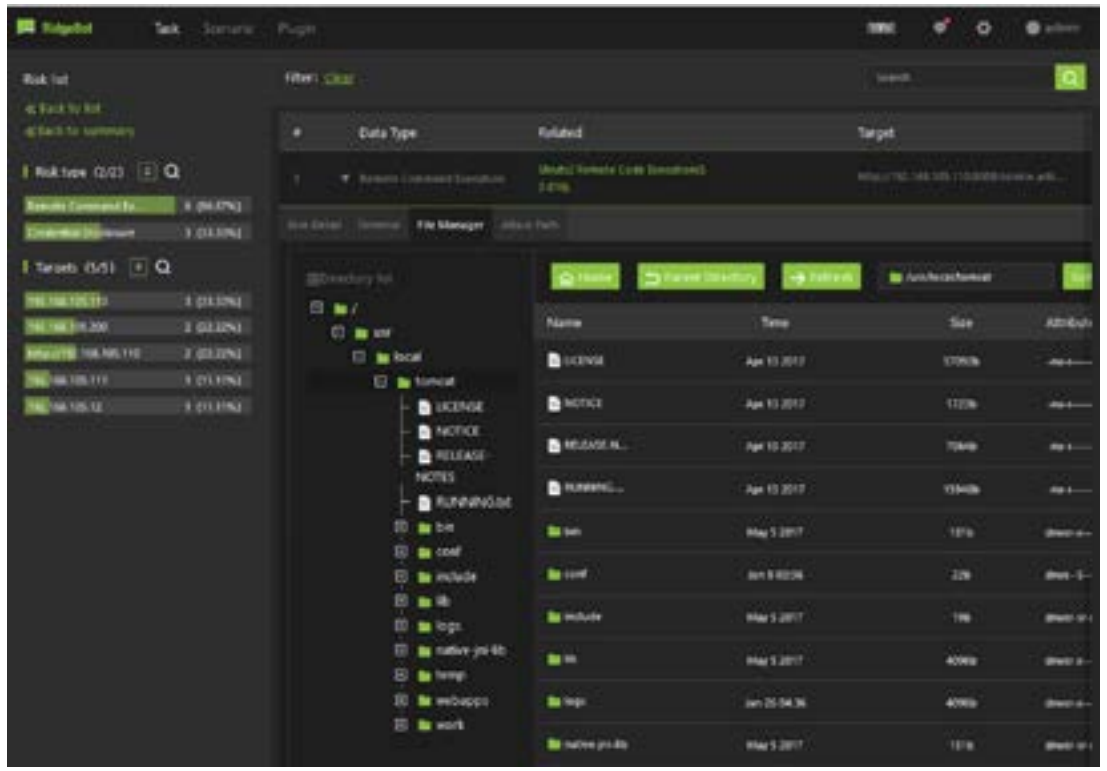
Attack sequence 6
Impact target: http://192.168.105.110:8008/cookie.action
Current User: root
OS: linux
shell type: Host shell

Attack sequence 1
Find 192.168.105.110 target

Attack sequence 3
Find the attack surface of the site
Site title: S2-008
Site address: http://192.168.105.110:8008/

Attack sequence 5
Found Struts2 Remote Code Execution(S2-016) vulnerability
Targets: http://192.168.105.110:8008/cookie.action

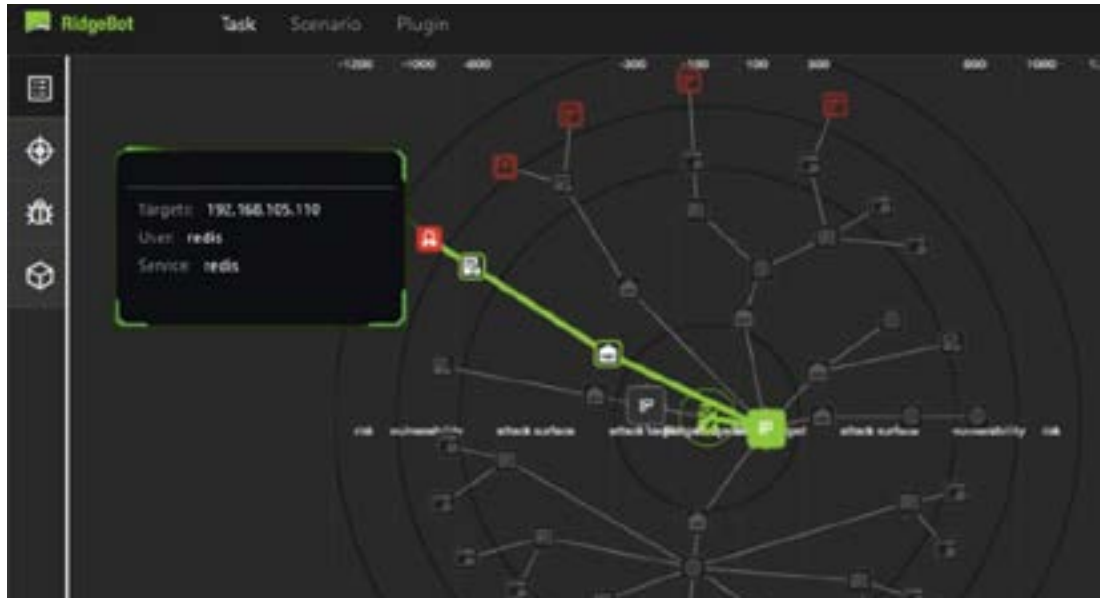
For Struts2 exploits, RidgeBot can harvest the file directory of the target host. A successful RidgeBot exploit of a Struts2 vulnerability is given in the Risk Table, showing that the host target was entered and its file directory is visible to RidgeBot.



Weak Password / Credential Disclosure

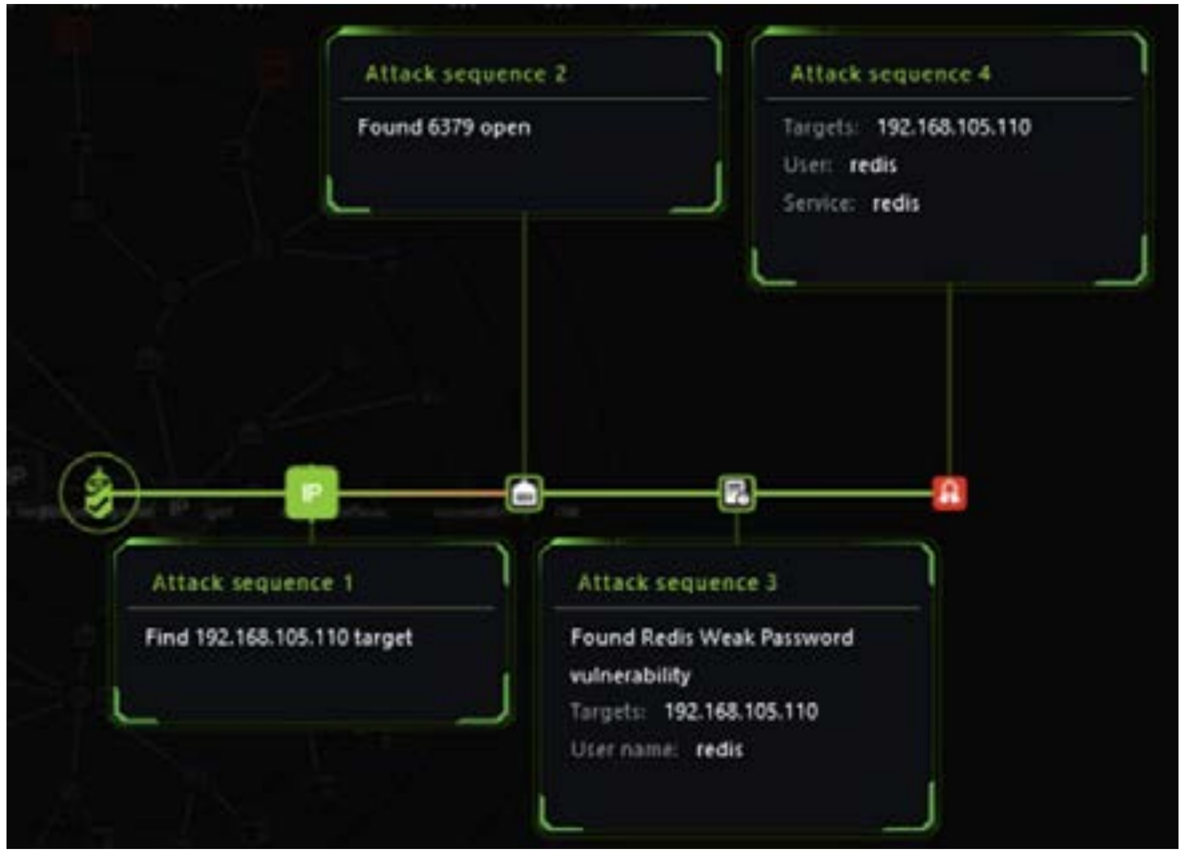
There are numerous known vulnerabilities related to weak passwords, or credential disclosure, in the industry, including those associated with SSH, Redis, SQL Server, SMB and Microsoft Remote Desktop Server. Some of the exploits relate to credential disclosure, others to RCE opening up "wormable" opportunities where malware can propagate from one vulnerable computer to the next, in a similar manner to how WannaCry ransomware propagated.

RidgeBot can scan your network, devices and servers to detect a cross-section of weak password vulnerabilities in your environment. RidgeBot further launches an attack against the target device by exploiting the weak password vulnerability found. In the sample Ridgebot attack against IP 192.168.105.110 shown below, a Redis weak password vulnerability was successfully penetrated (red box at the outer edge).



Targets: 192.168.105.110
User: redis
Service: redis

Drilling down on the exploit-path (green boxes) to the compromised target machine (red box), discloses the attack path the threat actor exploited to reach the target.



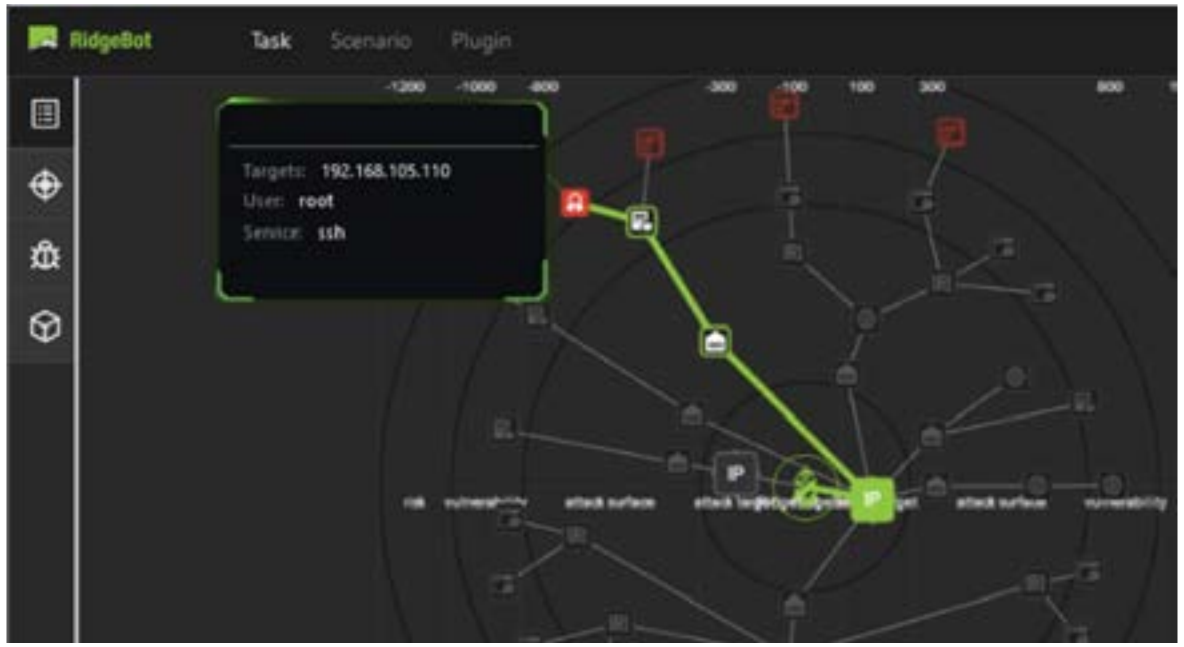
Attack sequence 1
Find 192.168.105.110 target

Attack sequence 2
Found 6379 open

Attack sequence 3
Found Redis Weak Password vulnerability
Targets: 192.168.105.110
User name: redis

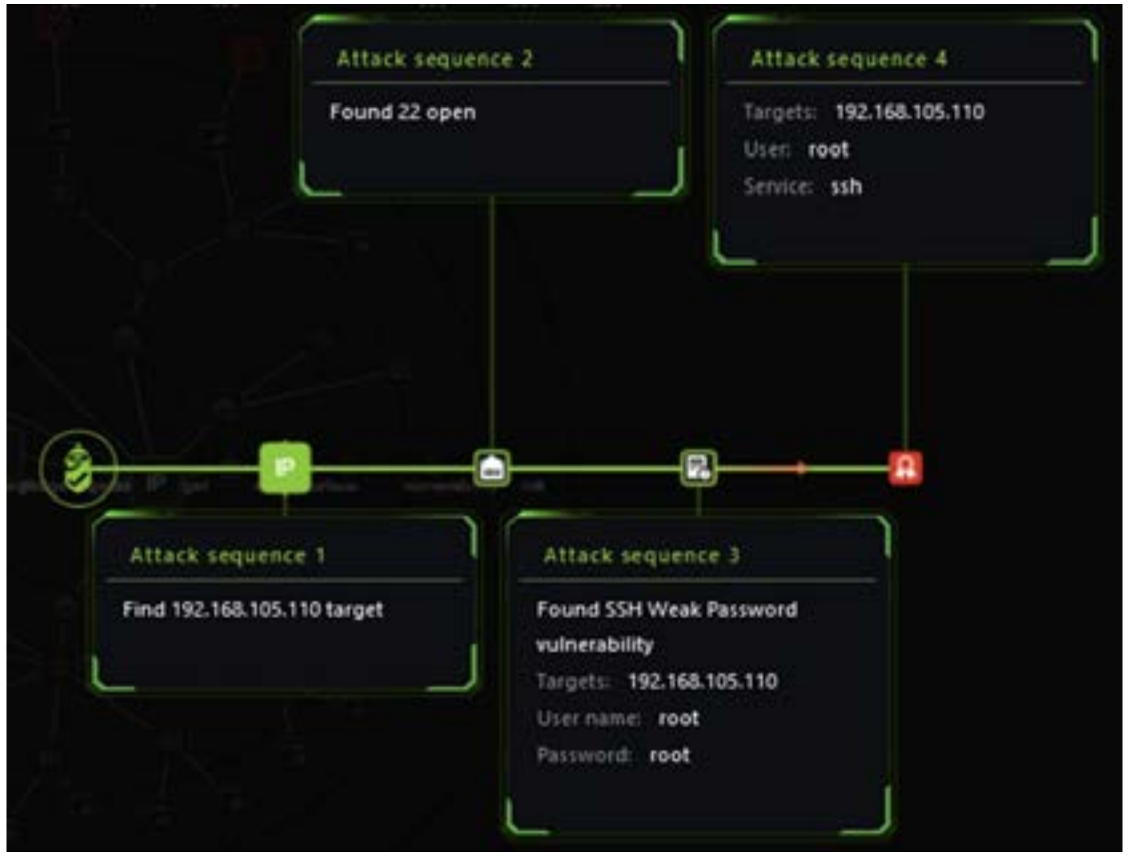
Attack sequence 4
Targets: 192.168.105.110
User: redis
Service: redis

In an example Ridgebot scan and attack against IP 192.168.105.110 shown below, an SSH weak password vulnerability was penetrated (red box at the outer edge).



Targets: 192.168.105.110
User: root
Service: ssh

Drilling down on the exploit-path (green boxes) to the compromised target machine (red box), discloses the attack path the threat actor exploited to reach the target.



Attack sequence 2
Found 22 open

Attack sequence 4
Targets: 192.168.105.110
User: root
Service: ssh

Attack sequence 1
Find 192.168.105.110 target

Attack sequence 3
Found SSH Weak Password vulnerability
Targets: 192.168.105.110
User name: root
Password: root

File Uploads

File upload vulnerabilities use files to insert malicious code triggering RCE on the target platform.

- **Local file upload vulnerability:** An application allows a threat actor to upload a malicious file directly, which is subsequently executed.
- **Remote file upload vulnerability:** An application leverages user action to fetch a file from a remote site on the Internet and store it locally to be executed at a later time.

RidgeBot can scan your network, devices and servers to detect numerous file upload vulnerabilities in your environment. Some of the more recent ones are listed below; RidgeBot's scanning plug-ins also cover numerous additional CVEs.

- VMware vCenter Server File Upload (CVE-2021-22005)
- WordPress File Manager older than 6.9 File Upload (CVE-2020-25213)
- WordPress File Upload Directory Traversal (CVE-2020-10564)
- Apache Tomcat JServ File Inclusion (CVE-2020-1938)
- Apache Tomcat PUT Method Write File (CVE-2017-12615)
- Oracle WebLogic Server Remote Code Execution (CVE-2021-2109)
- Oracle WebLogic Server Console Permissions Bypass (CVE-2020-14750)
- Oracle WebLogic IIOP Deserialization (CVE-2020-2551)
- Oracle WebLogic Remote Code Execution (CVE-2020-2883)

Deploy Ridge Security's RidgeBot: Demo

Once a threat actor has infiltrated your network and progressed to establish a foothold inside your assets, it is often too late to stop the damage. It is therefore imperative to keep threat actors from compromising your assets by keeping them from finding any opening through which to enter your network and assets.

RidgeBot contains critical scan and exploit capabilities specifically developed to combat vulnerabilities leading to targeted ransomware attacks. Contact us today for a demo on how RidgeBot can help your organization survive these dangerous times.

Ridge Security Technology Inc. www.ridgesecurity.ai