The Ransomware Rampage of 2020—and How to Survive 2021

RIDGE SECURITY

In 2020, ransomware yielded enough damage to solidify its position as a boardroom-level risk.

The Ransomware Rampage of 2020—And How to Survive 2021

A ransomware attack is a form of blackmail, and payouts have increased dramatically in 2020. It often seemed that every other day news broke from somewhere around the globe about yet another business affected by a ransomware attack that resulted in devastating consequences, extortion and ever larger payouts.

In 2020, ransomware yielded enough damage to solidify its position as a boardroom risk. Every aspect of the attacks is on the increase.

- The number of victims
- The number of payouts
- The amount of the payouts
- The damage to organizations
- Extortion for stolen data, in addition to the ransom for decrypting data

Blackfog reports that “Ransomware cyberattacks are a big business… research anticipates a business is attacked by a cybercriminal every 11 seconds and damage costs from these attacks will hit around [US]$20 billion by 2021.” 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.

Ransomware Trends

Several trends are leading to the rapid rise in both the frequency and size of attacks in 2020. Threat actors are also adjusting their playbook for larger and more assured payouts.

Trends Fueling the Increased Incidence of Ransomware Attacks

Business and industry trends have dramatically increased the attack surface of small-businesses, enterprises and government networks. Other trends have opened new opportunity.

- **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 needs at pay-as-you-use rates instead of heavy capital infrastructure investment.
- **COVID-19 Pandemic and Work-from-Anywhere:** The global response to the pandemic caused a momentous and sudden shift to a majority work-from-anywhere (WFA) professional workforce. Urgent organizational efforts to maintain business continuity during COVID-19 lockdowns additionally accelerated the already strong trend in cloud migration. Together, the cloud and WFA trends have dissolved the traditional hard enterprise network perimeter, substituting it with a software-defined perimeter (SDP) that runs along every surface of the network open to Internet access. Businesses are struggling with the ever-changing abilities and technologies to properly secure this new soft perimeter and WFA access via the Internet.
- **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 also led to a significant increase in the sophistication, severity 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.

  Following the same ease-of-deployment-with-limited-skill-needed path that SaaS, IaaS and PaaS have capitalized on, RaaS has now also moved to the cloud where highly customizable ransomware kits, purchased on the dark web, can 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 and Phishing:** This has long been the most successful initial entry-point for malware, but the COVID-19 pandemic has accelerated this trend with many new opportunities by preying on human fear as well as exploiting vulnerabilities opened by WFA setups. Threat actors pose as organizations that provide COVID-19 information, statistics, government economic-relief programs, personal protective equipment, or vaccine information.

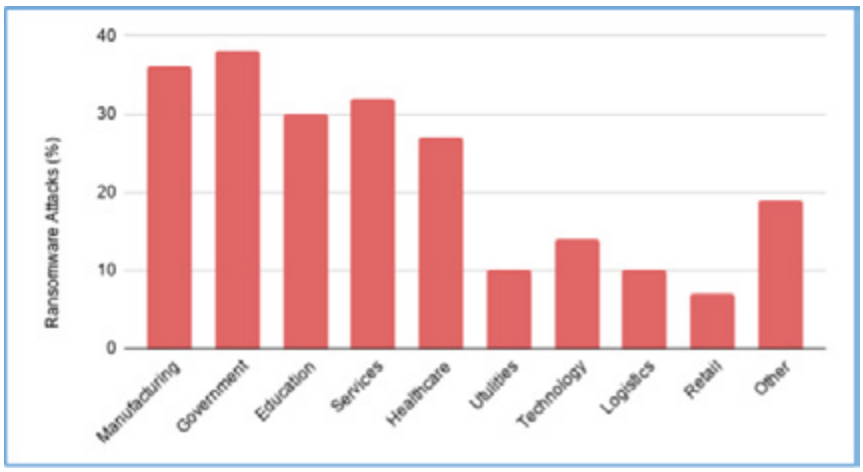
- **Bitcoin Payments:** The growing popularity and availability of crypto-currencies such as bitcoin offer payment methods with no traceability, no option to dispute, and un-cancellable transactions.

Trends in Ransomware Attack Approaches

Ransomware still occasionally targets consumers, but the vast majority of attacks have shifted to **focus on corporate and government targets**. The initial asset infiltration is almost as easy and the payout opportunities are enormous.

In 2020, threat actors have specifically targeted large organizations, and often those with **regulatory exposure**. The prospect of regulatory fines and reputation damage resulting from publicly exposed data privacy violations significantly increased the success rate of payouts, as well as the payout amounts.

SOCRadar Labs reports that the industries most affected by ransomware in 2020 are manufacturing, government, and professional services; organizations particularly averse to downtime.



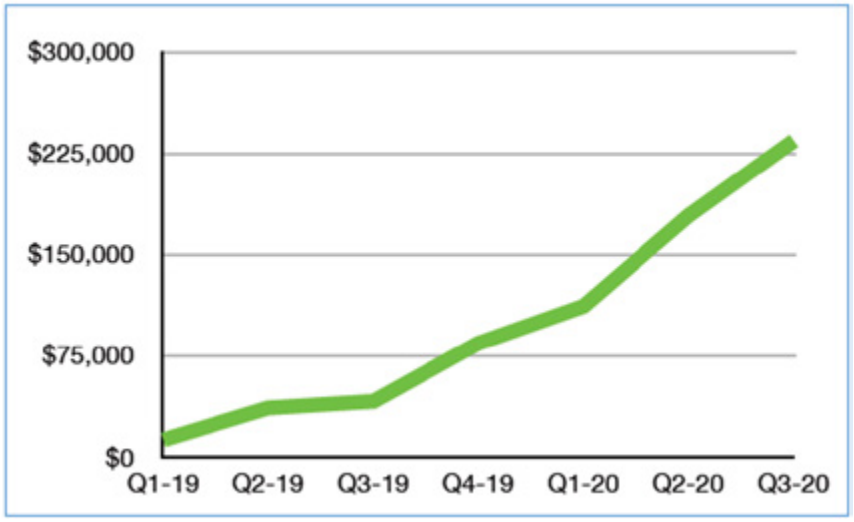
Ransomware has seen considerable **growth in virulence**, and—empowered by RaaS—**a larger population of threat actors** who can target a larger number of victims.

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 also 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 have also taken advantage of the fact that **businesses are distracted during the COVID-19 pandemic**. While emergency network and compute re-engineering is being done to ensure business continuity, the security vulnerabilities exposed by cloud migrations and WFA 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 previously exist.

Over the last two years, the **average ransom payout** has also increased significantly, as shown in Blackfog's Monthly Ransomware Report. The increase is partially attributed to attackers increasingly targeting larger companies.



Geographically, ransomware attacks mostly target **Asia, North-America and Europe**, although no country or organization in the world is exempt.

Traditionally, threat actors have targeted Windows systems as the largest **operating system installed base**, but as MacOS systems have gained market share in recent times, these platforms are increasingly targeted also.

A Coveware market report indicates 2020 Q3 statistics of the top 10 ransomware types.

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2020
1	Sodinokibi	16.2%	-
2	Maze	13.6%	-
3	Netwalker	9.9%	+1
4	Phobos	5.0%	-2
5	DopplePaymer	4.3%	New in Top 10
6	Snatch	4.0%	+2
6	Conti	4.0%	New in Top 10
8	Lockbit	3.6%	+1
9	Dharma	2.3%	-4
10	Nephilim	2.0%	New in Top 10
10	Avaddon	2.0%	New in Top 10

Trends in Ransomware Tradecraft

Presenters from Mandiant/FireEye at the BlackHat Europe Virtual Event held in December 2020 discussed the improvements and changes to ransomware tradecraft they observed in 2020.

- 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

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. General recommendations to minimize damage from a ransomware attack include:

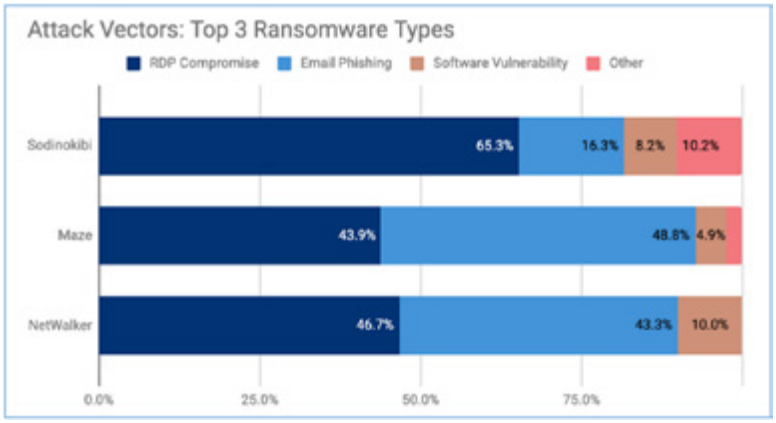
- Establish and maintain offline backups, and regularly test these to ensure systems can be rebuilt successfully.
- Employee education on social engineering and phishing strategies.
- Establish a strategy to prevent unauthorized data theft—especially where large amounts of data are stored or uploaded 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.
- Ensure all operating systems have up-to-date patches, and install antivirus software everywhere.

Commonly Used Techniques and Operating Modes

Most ransomware attacks use a small number of common infection vectors.

- **Phishing:** Malicious email attachments, also termed “malspam”.
- **Remote Desktop Protocol (RDP):** Network intrusion through unsecured ports and services.
- **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).

A Q3-2020 Coveware report provides details of the infections vectors of different ransomware types.



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 3.2

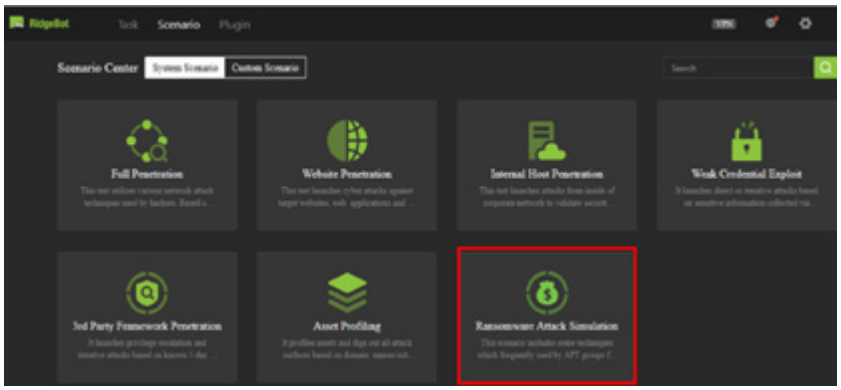
RidgeBot auto-discovers your assets, scans them, and then proceeds to exploit the vulnerabilities found just as a hacker would. In its report, it alerts you to the dangerous, successfully exploited vulnerabilities and also shows you the exact attack path that allowed the asset to be compromised. With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

RidgeBot 3.2 Ransomware Protection

Release 3.2 features a new template specifically focused on combating ransomware attacks. Initially this template includes:

- Scanning for 27 high-profile ransomware entry point vulnerabilities
- The ability to launch attacks to exploit these vulnerabilities
- Reporting in detail on exactly how successful exploitations were achieved

Definitions of more ransomware attacks will be added over time, and you can add these to your security arsenal by downloading periodic RidgeBot updates.



Running the RidgeBot 3.2 ransomware template 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, doing a software upgrade of a device, installing a patch on a device, changing scripts or information on a web server, or 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.

RidgeBot 3.2 Approach

The RidgeBot 3.2 ransomware template includes 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

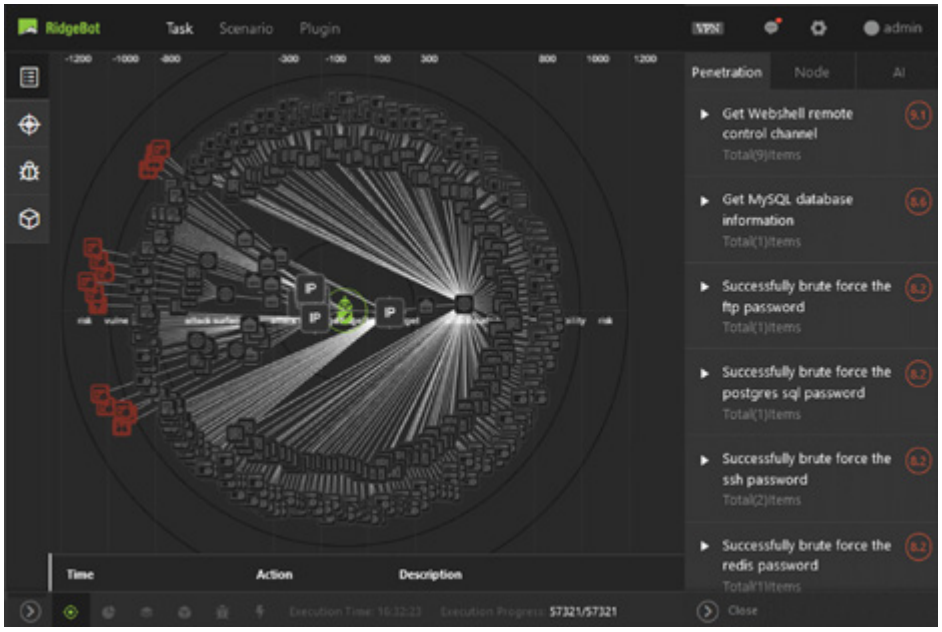
RidgeBot 3.2 Scope

RidgeBot scanning and exploitation cover technical vulnerabilities such as weak credentials, open ports, file uploads, WebLogic and Struts2 web application vulnerabilities. It can neither protect you against social engineering or phishing, nor with data that has already been encrypted by a ransomware attack. Instead, use RidgeBot to locate the vulnerabilities in your network to keep out ransomware intrusion.

If you consider your organization to be a possible or likely “target organization” for threat actors, then use the RidgeBot 3.2 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 will need additional tools to detect and correct the intrusion.

Combating High Profile 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.



The following sections provide details and examples of a number of high-profile, easily exploitable vulnerabilities that may exist in your environment. RidgeBot 3.2 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.

Remote Code/Command Execution: 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, including Windows Vista, Windows 7, 8.1, and 10, Windows Server 2008, 2012, and 2016. EternalBlue is also covered by CVE-2017-0143 to CVE-2017-0148.

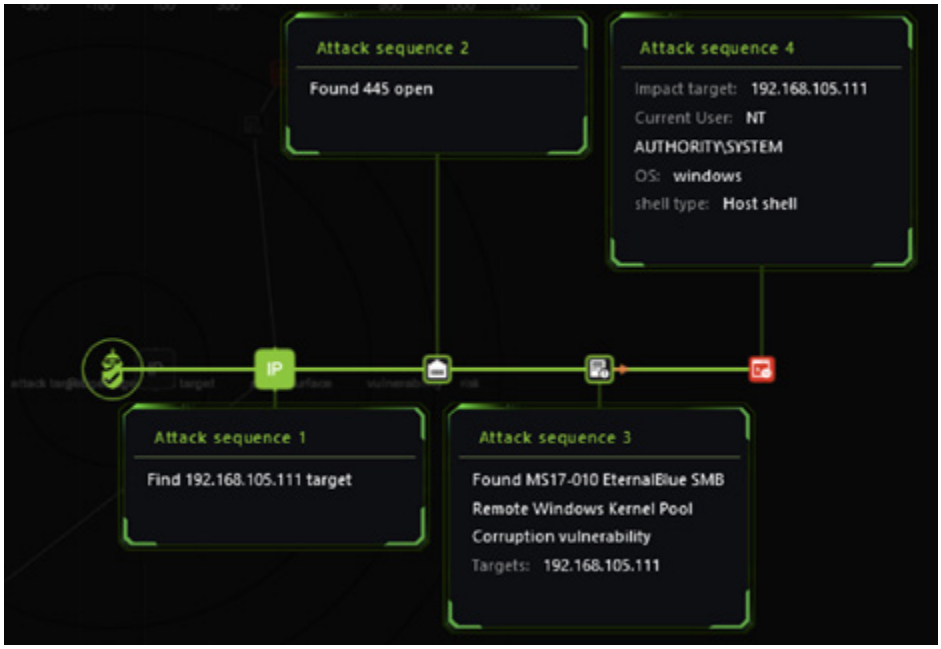
EternalBlue is an exploit allowing threat actors to gain access to a Windows asset, control the shell, and remotely execute arbitrary code by sending specially crafted packets to a server using Microsoft Server Message Block 1.0 (SMBv1). SMB is a network file sharing protocol to allow access to files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

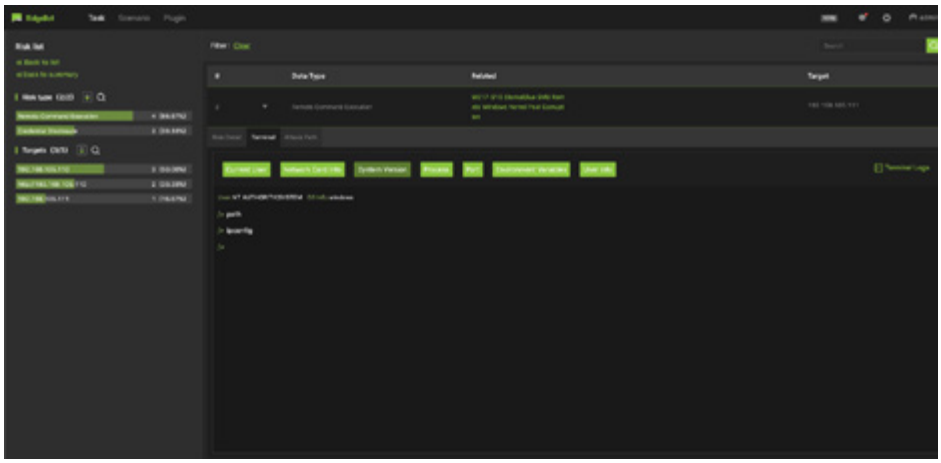
Despite the fact that the EternalBlue vulnerability—and Windows patches to counteract it—was already announced years ago in March 2017, there are still enough unpatched machines in early 2021 to make this exploit very attractive to threat actors.

RidgeBot 3.2 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 EternalBlue 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).

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.



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.



Remote Code/Command Execution: Struts2

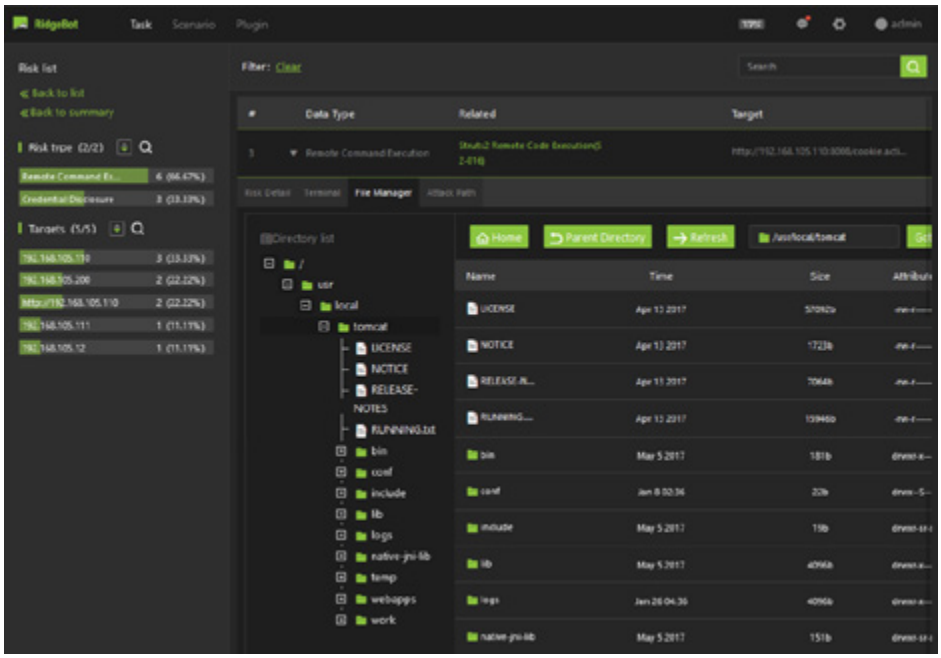
Apache Struts2 is a free, open-source web application (Model-View-Controller, or MVC) framework for developing cross-platform Java web applications. It has an extensible architecture using the Java Servlet API and REST, AJAX and JSON plugins to enable easy software development.

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 3.2 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).

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.

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 Attacks

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 3.2 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).

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.

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).

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.

WebLogic and Other File Upload Attacks

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 3.2 can scan your network, devices and servers to detect the following file upload vulnerabilities in your environment.

- Apache Tomcat PUT Method Write File (CVE-2017-12615)
- WebLogic Service Test Configuration Page Has Arbitrary File Upload (CVE-2018-2894)
- WebLogic XML Decoder Deserialization (CVE-2017-10271)
- Apache ActiveMQ Arbitrary File Writing (CVE-2016-3088)

Deploy RidgeBot 3.2 Ridge Security 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 3.2 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.

Company Profile

Ridge Security delivers ethical, efficient and affordable pen testing solutions to enterprises, small and large. We ensure our customers stay compliant, alerted and secure at all times in the cyber world. The management team has many years of networking and security experience. Ridge Security is located in the heart of Silicon Valley and is expanding into other areas including Latin America, Asia and Europe.

RidgeBot, a robotic penetration testing system, fully automates the testing process by coupling ethical hacking techniques to decision-making algorithms. RidgeBots locate, exploit and document business risks and vulnerabilities discovered during the testing process, highlighting the potential impact or damage.

Ridge Security Technology Inc.
www.ridgesecurity.ai