

# Malware Threat Report 2021

BeyondTrust Labs Analysis of  
Ransomware and Phishing Trends  
& How to Mitigate Them

**James Maude**  
Lead Cybersecurity Researcher





## TABLE OF CONTENTS

<b>Executive Summary</b>	<b>3</b>
<b>Security Challenges of 2020-2021</b>	<b>4</b>
The Increased Attack Surface - Bringing Threats Home	4
The New Perimeter	7
More Privileges, More Problems	9
Privileged Application Vulnerabilities	11
Summary of Security Challenges	13
<b>Maturity of the Malware Ecosystem</b>	<b>14</b>
Human-Operated Ransomware	16
<b>BeyondTrust Malware Labs - Analysis of Malware Threats</b>	<b>21</b>
Overview of Malware Strains	22
Common Denominators	27
Most Common Techniques After Initial Malware Execution	29
Lab-Testing BeyondTrust Trusted Application Protection Against Top Malware Strains	31
Diving Into MITRE ATT&CK® Framework Definitions & Mitigations	34
T1047 Windows Management Instrumentation (WMI)	35
T1204.002 User Execution: Malicious File	36
T1059.001 PowerShell used for initial execution	37
T1059.003 Windows Command Shell (CMD)	38
Other Techniques	39
<b>The 5 Critical Steps to Complete Endpoint Security</b>	<b>40</b>
<b>Additional Resources</b>	<b>43</b>
<b>Appendix: Threat Samples Tested</b>	<b>44</b>

Note: The lab-based research in this report pertains only to Windows desktops and servers.



# Executive Summary

This research report provides insights and analysis into threats and privileged account misuse on Windows devices across the globe. This research is from the same BeyondTrust Labs team that publishes the annual [Microsoft Vulnerabilities Report](#).

**This report is based on real-world monitoring and analysis of attacks between Q1 2020 and Q1 2021 discovered in the wild by the BeyondTrust Labs team,** with collaboration from customers and incident response teams using BeyondTrust's products. In addition to general insights into the threat landscape, the report also dives into reoccurring threat themes and maps out Tools, Techniques, and Procedures (TTPs) against the [MITRE ATT&CK® Enterprise Framework](#).

BeyondTrust Labs explored the 58 techniques in the MITRE ATT&CK Framework lists for Cobalt Strike (threat emulation software), and **66% of the techniques either recommend using Privileged Account Management, User Account Management, and Application Control as mitigations or list Administrator / SYSTEM accounts as being a prerequisite for the technique to succeed.** Therefore, the control of privileges and application execution is a key defensive measure in mitigating Cobalt Strike and tools/malware with similar capabilities, by reducing the attack surface and denying code execution and privileged rights.



## KEY FINDINGS

- 1 Absent the right protection, malware will disable endpoint security controls and undermine your security investment.
- 2 We are observing a growing trend in the use of native tools to perform fileless attacks in the initial stages until a strong foothold and persistence mechanism is established and security controls have been disabled.
- 3 The MITRE ATT&CK Framework provides an effective way to distill a wide range of malware strains and cyberattacks into component techniques, which can then be mitigated.
- 4 BeyondTrust's out-of-the-box policies proactively disrupted all 150 different, common attack chains tested in our analysis.
- 5 Removal of admin rights and implementation of pragmatic application control are two of the most effective security controls for preventing and mitigating the most common malware threats.



# Security Challenges of 2020-2021

## The Increased Attack Surface: Bringing Threats Home

Security staples such as network monitoring and firewall technologies are becoming less effective as the perimeter shifts from the corporate office to the home office, or “work from anywhere” for that matter.

Over the past two decades, organizations invested significantly in shoring up their cyber defenses. Some of these investments have been rendered far less effective, even obsolete, due to the changes ushered in by the pandemic.

Email fatigue is greater than ever. The daily communications that once happened in-person, or over the office phone, have shifted increasingly to emails, online meetings, and other communication tools.

This means that users are not only seeing higher volumes of emails, but also receiving emails from a wider range of sources, such as:

- ▶ Colleagues they have never met
- ▶ Prospective suppliers
- ▶ New clients
- ▶ Other departments about policies, tools, and information needed to support home working

Despite the rise of modern collaboration software, most office communication still revolves heavily around sending and receiving emails with documents, links, or other attachments. For example, an HR team expects to receive resumes, and a finance department expects invoices or contracts.

The expectation of receiving legitimate communications via email—often from sources unknown or unanticipated—makes it easy for an attacker to tailor an email phishing campaign and achieve a high success rate. Departments with access to the most documents and data are often the most likely to fall victim to phishing efforts, subsequently leading to a ransomware or other malware attack.

**Figure 1** Example of COVID-19 themed phishing email linking to malicious Word document





Consequently, threat actors launched highly successful campaigns that use targeted phishing emails to socially engineer the overwhelmed remote worker into entering their credentials or opening an infected document.



➤ In BeyondTrust Labs, we observed a **200% increase** in phishing emails with the majority being COVID-19 themed.

The threat actors sending emails impersonated a variety of government and non-government organizations, from the World Health organization (WHO) and Center for Disease Control (CDC) to government departments and pharmaceutical companies.

These email campaigns prompted the Department of Homeland Security (DSH), Cybersecurity & Infrastructure Security Agency (CISA) and the World Health Organization (WHO) to issue communications warning users of the risks. The United Kingdom National Cyber Security Centre also launched a campaign to be “Cyber Aware” following the takedown of 2,000 scams, including 471 fake online shops for COVID-19 related services.

### WHO Communication Warning Users of Phishing Techniques

“The World Health Organization will:

- ▶ **Never** ask for your username and password to access safety information
- ▶ **Never** email attachments you didn't ask for
- ▶ **Never** charge money to apply for a job, register for a conference, or reserve a hotel
- ▶ **Never** conduct lotteries or offer prizes, grants, certificates or funding through email





## The New Perimeter



*“Just like the ice wall in Game of Thrones, organizations spent years building a technological perimeter wall to keep threats out. Despite cries that “the perimeter is dead,” they have continued to place a lot of faith (and investment) in it. The rapid transition to remote working, and the sudden dissolution of the perimeter, has forced an abrupt shift to focus on securing identities and end-user devices. IT departments are under pressure to upgrade capacities fast and this results in changing or replacing existing systems with little time to do thorough security tests. Vulnerabilities in the remote access infrastructure and access protocols may remain undetected and can be exploited in cyberattacks.”*

[International Monetary Fund:  
Cybersecurity of Remote Work During the Pandemic](#)

To adapt to social distancing initiatives or work from home policies, **businesses were forced to accept unprecedented risks that would have been inconceivable a few months prior**, just to continue operating and keep users productive.

In some cases, old desktop machines that no one ever imagined leaving the corporate network, were being loaded into cars and taken home to potentially vulnerable networks that they were never intended to join.

A wide range of remote access tools and cloud services were hastily spun up, sometimes overnight or over a long, sleepless weekend.

In many cases, due to the speed of the deployments, users were all given broad access to data and systems as business erred on the side of freedom and flexibility to ensure that users were able to work remotely.



Attackers overwhelmingly seek out the easy targets that will yield a fast payday. Thus, cyber criminals quickly capitalized on this sudden shift, rapidly identifying that not only had the attack surface vastly increased, but so did the access to data and systems. One of the outcomes of these factors was reflected in the surge of successful ransomware campaigns, as attackers were able to land and expand with newfound ease. Since the pandemic, there has been a third more ransomware families and 560,000 new pieces of malware detected every day (DataProt, 2021).



➤ BeyondTrust Labs has also witnessed an increased in specialist Ransomware-as-a-Service (RaaS) operators, which not only provide services that **lower the technical barriers** for would-be cyber-criminals but are also far more capable of taking down large enterprises.

Many organizations who previously had robust monitoring in place on the internal network—helping to identify malware traffic and lateral movement—have been blind to the new and evolving attack techniques. This is because so many endpoints now operate partially or fully outside of the network. To compound this problem, there was a nearly **900% surge in fileless malware attacks** (Internet Security Report for Q4 2020, WatchGuard Technologies) which often involve attackers exploiting native applications, like PowerShell, to perform tasks. This reduces the chance of detection as many solutions are looking for new applications appearing rather than existing, legitimate, tools launching.

In this environment, it's hardly surprising that multimillion dollar ransoms are now commonplace. These ransoms are not just quick cash payouts, but seed rounds for the ransomware operators, who continue to invest in better infrastructure and leveraging zero-day exploits.





## More Privileges, More Problems

Over the past few years, most organizations have been advancing toward a least privilege approach, where users are only allocated the privileges/privilege access they need to do their role. In many industries, this is now mandatory (NIST, PCI, HIPAA, etc). Due to the effectiveness of this security control, it is expected that companies in other industries will follow.

**Supporting the newly remote workforce presented organizations with many challenges around privileged access.** For instance, seemingly trivial tasks, like installing printer drivers for the device in the home office, or the software needed for a new wireless headset, or updating the local time on a laptop, required local admin rights that users didn't have. To continue functioning without overwhelming support desks with calls and tickets, many organizations gave users access to local admin rights on a temporary or permanent basis, vastly increasing the security risk.

The International Monetary Fund (IMF) addressed this topic in a special series of notes warning of the potential cybersecurity risks brought about by remote working during the pandemic. This increased pervasiveness of local admin rights has made it significantly easier for common malware strains to use simple Elevation of Privilege (EoP) techniques to not only gain access to privileges on the system, but also use these privileges to disable or bypass existing security controls.

Thus, it's critical to remove local admin rights and apply more granularity around privileged access security controls.

“We were up against the clock on this one and ended up issuing work from home laptops with local admin rights for the old desktop user groups. We also had to react to an influx of support calls by granting temporary admin privileges to our existing laptop user groups. This was all because we didn't have a solution in place at the time. Privilege Management has quickly become our top priority.”

**Head of IT Ops,  
Engineering Firm**



“Employees should not have administration rights on firm-owned notebooks, security hardened configurations and up-to-date endpoint security solutions should be in place, **connection security parameters should be set according to good practices and should be locked, and the corporate remote access infrastructure should be tightly controlled.**”

[International Monetary Fund:  
Cybersecurity of Remote Work During the Pandemic](#)





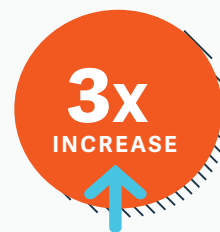
## Privileged Application Vulnerabilities

Alongside the increase in users with admin rights, we have observed a rising trend in software that does not properly manage privileges.

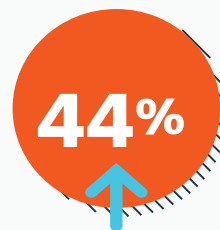
The 2021 edition of the BeyondTrust Labs annual [Microsoft Vulnerabilities Report](#) found the following:

- ▶ Elevation of Privilege (EoP) vulnerabilities increased **3x** from 2019 to 2020
- ▶ These accounted for **44%** of the 1,268 critical Microsoft vulnerabilities surveyed in 2020
- ▶ Remote Code Execution (RCE) was the next highest category (**27%** of the critical vulnerabilities)

The issue of improper privilege management has been highlighted by MITRE, who included CWE-269 – Improper Privilege Management in their “2020 CWE Top 25 Most Dangerous Software Weaknesses.”



EoP vulnerabilities  
YoY 2019-2020



EoP YoY increase  
2019-2020

### CWE-269:

#### Improper Privilege Management

*The software does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor.*

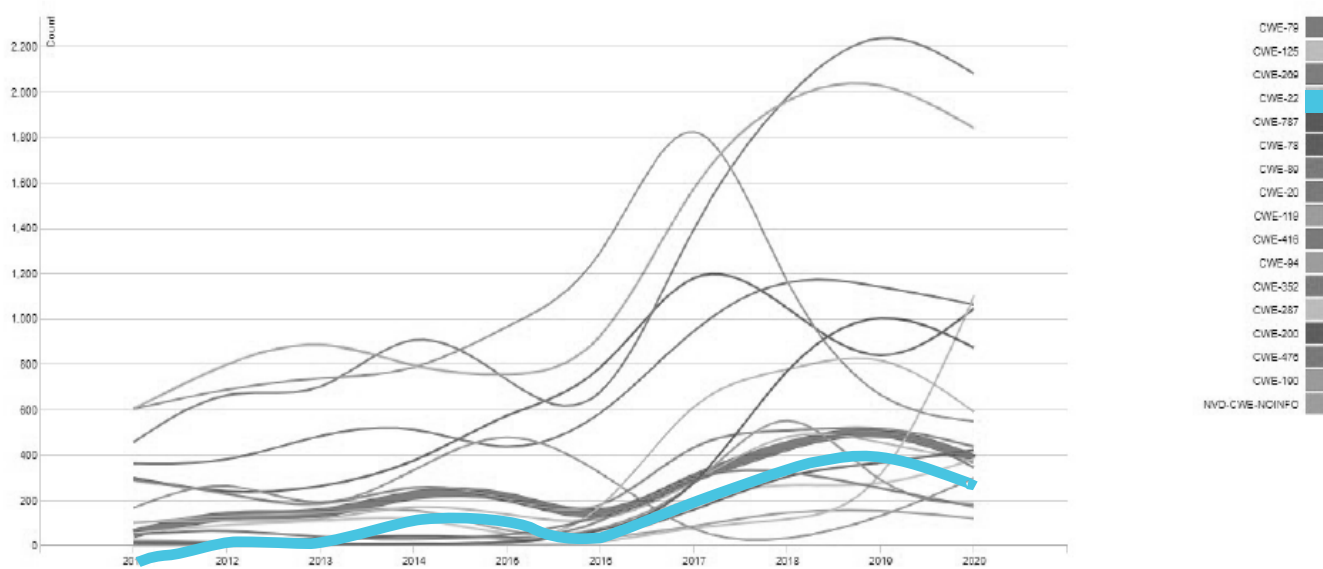
MITRE ATT&CK  
Framework



As shown in the chart below this weakness has been trending upwards almost exponentially since 2016.

Thus, it is more important than ever to control the privileges granted, not only at the user level, but at the application level, to prevent that sphere of control being created for a threat actor.

### Vulnerability Type Change by Year



However, the issues of improper privilege management are not just a Windows problem, as the data shown above tracks common weaknesses against a variety of software and operating systems. **While it is not always possible to control how the software itself handles privileges, the principle of least privilege (POLP) can be directly applied to the application to control risk.** From restricted tokens, to controlling child process inheritance, there are a variety of ways a robust endpoint privilege management solution can mitigate the risk of improper privilege management by applications.

**Figure 2** CWE-269 Improper Privilege Management has been vastly increasing since 2016

Source: [NIST](#)

*This visualization is a slightly different view that emphasizes how the assignment of CWEs has changed from year to year.*



## Summary of Security Challenges

**In 2020, the attack surface expanded massively due to:**

- ▶ The expansion in use cases for granting access to privileges
- ▶ An increase in software being vulnerable to dangerous vulnerabilities
- ▶ The widespread use of remote access that resulted from a massive shift to remote working

Attackers shrewdly exploited these new cyber exposures, often using elevation of privilege attacks and sophisticated malware campaigns, frequently playing on the emotions and fears of users.

Threat actors work ceaselessly to evolve their operations and have matured significantly over the past year. In our next section, we will explore the continuing evolution of the cybercrime industry.



## Maturity of the Malware Ecosystem



➤ Parallel to legitimate software companies and the trend towards SaaS, **threat actors are shifting to Malware-as-Service (MaaS) models** with specialists emerging in different areas, including enterprise credential sales, initial access to a target organization, lateral movement capability, or payload delivery.

As with any growth industry, we have seen a lot of changes in malware ecosystems and their economic models.

Today, there are often many different pieces of malware that come together in an attack. A modern ransomware attack could be comprised of multiple threat actors, tools, and platforms.



***For example:***

- ▶ Threat actors rent the Necurs botnet and use it to distribute malicious spam
- ▶ Spam contains malicious documents that launches Trickbot
- ▶ Trickbot is used to harvest credentials, access emails, and for lateral movement across the network
- ▶ With widespread compromise of the target network, the threat actor sells backdoor access to the network to the highest bidder
- ▶ The buyer then deploys RYUK ransomware via the Trickbot command and control servers

This specialization not only drives innovation through competition, but also reduces the threat actor's risk. If one part of the chain is taken down, the other parts can quickly shift to another supplier.

Alternatively, if you're a threat actor looking to avoid being blocked by antivirus (AV) tools, then you can just buy access to systems where Trickbot has already breached the network and disabled the AV software.

**This approach makes modern malware considerably more resilient to takedown attempts, while also setting the technical bar for illicit entry much lower.** After all, an attacker no longer has to be an accomplished developer, social engineer, or skilled hacker. They can now buy, rather than build, tools and use the MaaS platforms to orchestrate sophisticated malware campaigns.

In this chain of events, we can see several malware players and their tools within their own specialties. This modular approach allows the malware authors to focus on excellence in one area.



## Human-Operated Ransomware

As threat actors seek to maximize the disruption to organizations and extract the highest ransom payments, the ransomware model is shifting towards human-driven, enterprise-wide attacks.

Rather than create an automated worm that self-propagates across the network, **the latest generation of ransomware-as-a-service (RaaS) will tread lightly**, establishing a foothold in the network of a large organization.

Using common penetration testing tools – such as Cobalt Strike or PowerShell Empire – they then survey the network and spread using privilege escalations to gain control of critical systems and disable security controls, before finally encrypting key systems and exfiltrating data.

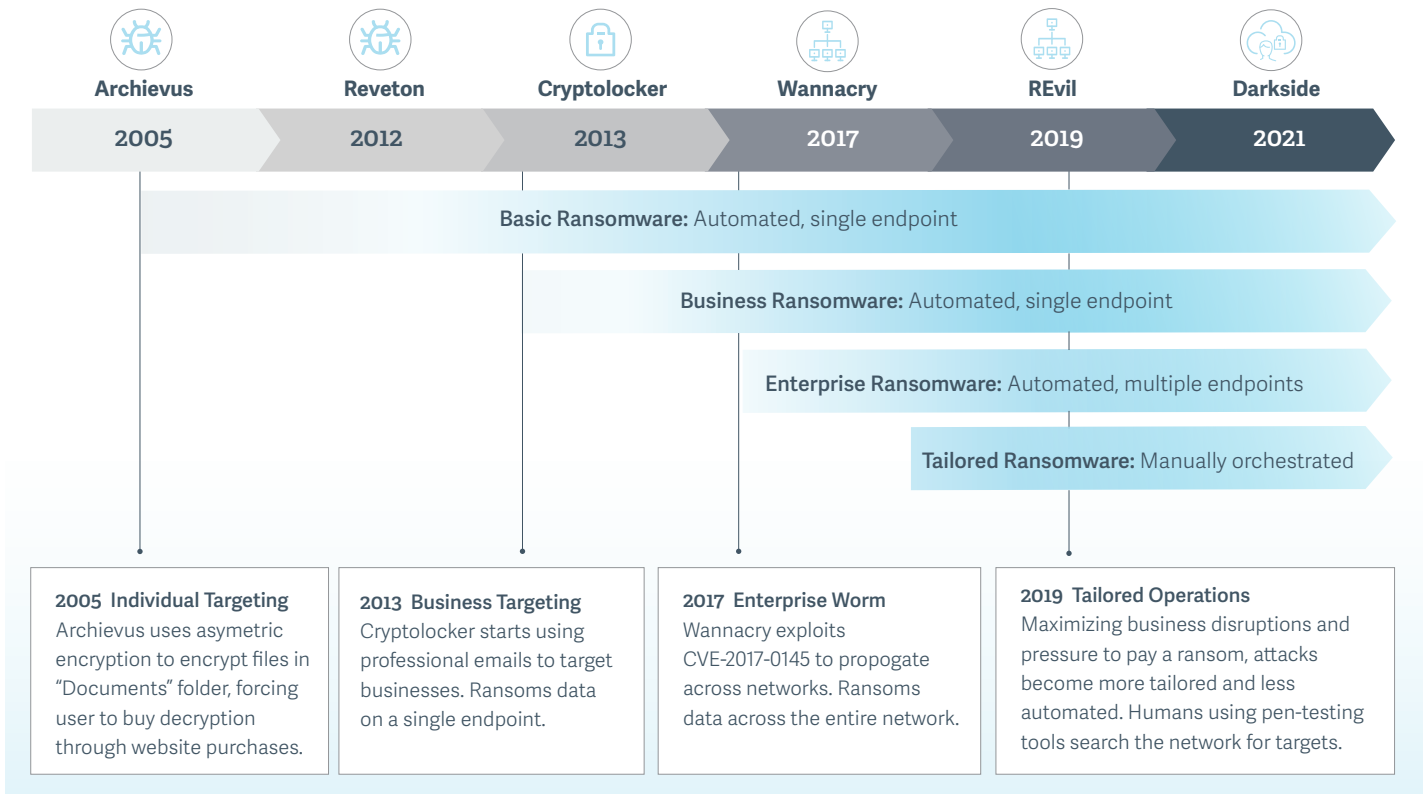
Human-operated ransomware campaigns pose a significant and growing threat to businesses and represent one of the most impactful trends in cyberattacks today.

In these hands-on-keyboard attacks, which are different from auto-spreading ransomware like WannaCry or NotPetya, adversaries employ credential theft and lateral movement methods traditionally associated with targeted attacks like those from nation-state actors.

[Human-operated Ransomware Attacks: A Preventable Disaster](#)



## The Evolution of Ransomware



Over the past 15 years, ransomware attacks have shifted from targeting a few file types in a single folder on one endpoint, to widespread encryption of entire networks of systems. While taking down a big network and many systems can result in a more devastating attack and greater business impact, it also lengthens the attack chain, providing more opportunities to detect and prevent the attack.

From a defensive point of view, this latest evolution of ransomware makes it far more difficult to identify attacks by using traditional detection tools, as they are less likely to use a generic payload. Instead, human-operated ransomware attacks involve a real person using professional tools.

**Figure 3** How ransomware has evolved as it seeks out more critical data and systems as higher value targets



This hands-on approach can wage a highly tailored attack on the target that frequently involves obfuscating code and leveraging fileless techniques to maintain a light footprint and to avoid triggering alarm bells while they explore the systems.

Fileless techniques may exploit native applications like PowerShell or .NET developer tools to run scripts and launch payloads, avoiding introducing new applications to disk that may be detected or blocked.

**Figure 4** Below, example of a human-operated ransomware campaign observed in the wild

### Human Operated Attack Chain

Attack Chain Phase	MITRE Framework	Example
<b>Access Environment</b>	T1566 Phishing	<b>Initial Access</b> Trickbot via phishing email
	T1548.002 UAC Bypass	<b>Execution &amp; Local Elevation</b> Cobalt Strike or PowerShell Empire
<b>Persist, Recon, Traverse and Spread</b>	T1134 Access Token Manipulation T1003 & T1003.001 Credential Dumping	<b>Credential Access</b> Using LaZange, Mimikatz or other tools
	T1055 Process Injection	<b>Privilege Escalation</b> Control over Valid Admin Accounts
	T1053 Scheduled Task/Job T1078 Valid Accounts: Domain Accounts	<b>Persistence</b> New Domain Admin (DA) Accounts
	T1087 Account Discovery T1033 System Owner/User Discovery	<b>Discovery</b> Recon and enumeration using Bloodhound
	T1035 Service Execution	<b>Lateral Movement</b> PsExec or other tools
	T1562 Impair Defenses	<b>Defense Evasion</b> Tampering with A/V & security services
	T1086 Data Encrypt for Impact	<b>Impact</b> Invoke Ryuk ransomware payload
<b>Execute Objective</b>		

#### The Role of Privilege Management for Windows

Prevents Powershell from being launched from a phishing attachment

Prevents access to local admin rights, mitigating credential access, privilege escalation and defensive evasion

Prevents malware payload executing



As shown in the previous page attack chain chart, there are many stages in a human-operated ransomware campaign as the attacker seeks deeper access and control of the network.



Starting from the phishing email, the attack will exploit privileges and the ability to execute applications like PowerShell to “land and expand,” **eventually leading to total compromise large enterprises.**

Professional tools, such as Cobalt Strike, offer an attacker several techniques for executing code, capturing credentials, and moving laterally within a network. Such tools are popular with threat actors. APT29, Wizard Spider, and Chimera are just a few of the cybercrime groups that have been observed using Cobalt Strike as part of their attacks.

MITRE has [mapped the functionality](#) of Cobalt Strike and recommends Privileged Account Management M1026 and Execution Prevention M1038 as mitigations against a range of the tool's techniques.

In fact, if we take a deeper look at the 58 techniques MITRE lists for Cobalt Strike, 66% of them either recommend using Privileged Account Management, User Account Management, and Application Control as a mitigation, or list Administrator / System accounts as being a prerequisite for the technique to succeed. Therefore, **the control of privileges and application execution is a key defensive measure** in mitigating this specific tool, and ones similar to it, through a reduction in the attack surface and denying code execution and privileged rights.

Trickbot, and the Ryuk operators, also take advantage of users running as local administrators in environments and use these permissions to disable security tools that would otherwise impede their actions.

[Human-operated Ransomware Attacks: A Preventable Disaster](#)



➤ While ransomware has clearly evolved, **the fundamental needs to execute code and leverage privileges have largely remained consistent.** Whether it is the basic ransomware hitting a single endpoint, or a sophisticated, tailored attack, the benefits of proactively reducing the attack surface by removing admin accounts and controlling application execution are universal.

When it comes to human-operated ransomware, one of the attacker's key objectives is to find accounts with local admin rights. Attackers exploit these accounts to disable security controls and steal credentials that allow them to move laterally, deeper and deeper into an environment.

The example attack chain shown in Figure 4 could have been thwarted at an early stage by simply preventing the phishing document from launching PowerShell and eliminating the local admin rights to prevent credential dumping.

We also want to highlight the importance of mitigating credential dumping techniques as these are often critical steps for an attacker to perform discovery, lateral movement, persistence, and defensive evasion.

**The attacker's goal is to "land and expand"—a simple path to privileged credentials makes this far easier to achieve.** When you mitigate the attacker's ability to execute and perform credential dumping, you don't just mitigate those techniques, but also a broad range of other ones that hinge on credential access to succeed.





## BeyondTrust Malware Labs

# Analysis of Malware Threats

### (May 2020 to May 2021)



➤ Phishing, social engineering, and drive-by compromise remain the most common initial access techniques seen by BeyondTrust Labs from May 2020 – May 2021.

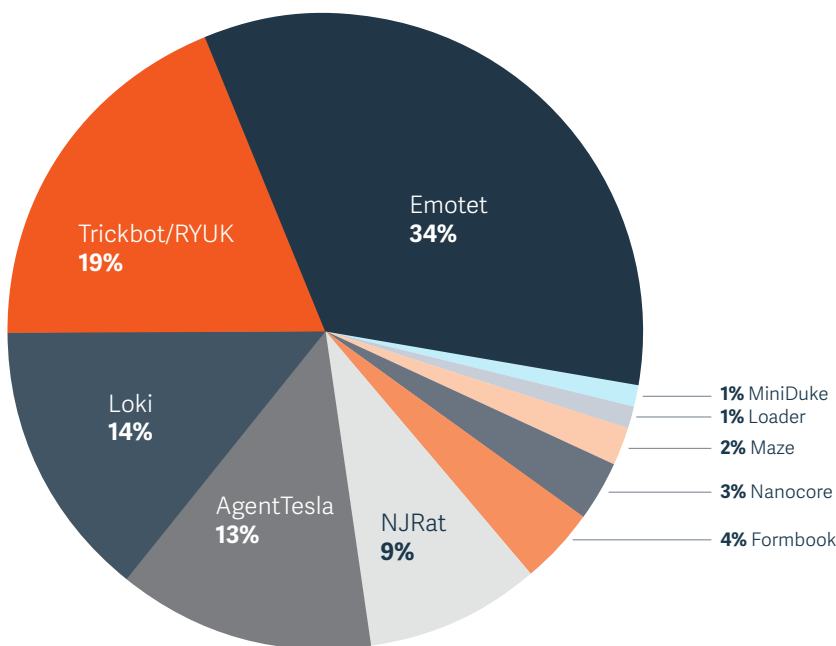
An uptick in ransomware delivered using RDP methods in 2020 was largely caused by unpatched systems, vulnerable to the BlueKeep exploits published in 2019, or simple misconfiguration. This is symptomatic of businesses overriding security concerns to ensure access and continuity, which leads to systems running RDP being directly exposed to the internet.

BeyondTrust helps businesses overcome this challenge with our [Secure Remote Access](#) solutions, which apply robust privileged access security controls around remote access sessions, and help organizations enable zero trust principles.

Given that this report is focused on endpoints and that remote access vulnerabilities could warrant an entire report on their own, we will cover the latter in more detail in later publications.



## Overview of Malware Strains



**Figure 5** Most common malware strains observed by BeyondTrust Labs Q1 2020 – Q1 2021

As illustrated in the figure above, Emotet and Trickbot dominated the threat landscape from Q1 2020 – Q1 2021. Emotet's success attracted the interest of international law enforcement agencies, leading to a large-scale takedown led by EUROPOL in early 2021.

While this takedown significantly slowed Emotet infections for a few weeks, Emotet-style variants quickly emerged. Many other malware strains have also adopted the same techniques that made Emotet so successful.

While many of these malware families are highly modular and offer a variety of functions, the primary use cases remain ransomware attacks and data theft, which often go hand-in-hand.



When an organization is compromised, the attacker will typically see if they can access data with black-market value, such as banking information or trade secrets. If there is no immediate black-market value to the data, or the attacker has exhausted it, they will then turn to ransomware to further monetize the data they have accessed.

Modern RaaS threat actors are extremely efficient in extracting the most value from their ill-gotten gains. Today, ransomware attacks frequently go beyond merely encrypting data, to also exfiltrating and extorting data.

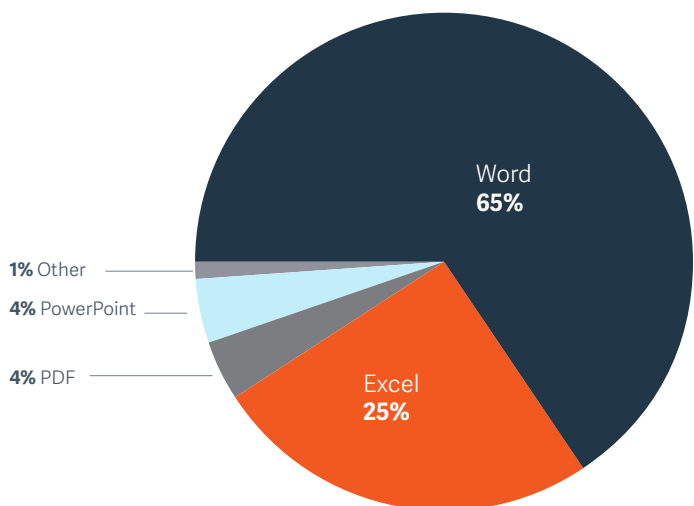
**In 2020, the BeyondTrust Labs team observed the following extortion tactics:**

- ▶ Ransomware demands for encryption at rest on the victims' systems
- ▶ Data exfiltrated to "bulletproof" cloud hosting with threat of publication if a ransom isn't paid
- ▶ Partners and clients of victims being threatened with publication if a ransom isn't paid
- ▶ Details of large breaches sold to unscrupulous traders in order to short stock prices ahead of a public announcement

Ransomware strains have clearly evolved a long way from asking for a few dollars for your local documents folder and now present a quadruple threat to victims.

These tactics came to light with the Colonial Pipeline attack and other victims of the Darkside group, who spelled out the data they had accessed and the threat of publication on their own nefarious website.

As with previous years, Word documents remain the predominant attack vector followed by Excel, while PDF based attacks continue to decrease as the number of vulnerabilities in PDF readers has reduced over time.



**Figure 6** Most common initial access vectors observed in 2020 – 2021

Attackers continue to innovate how they deliver these files and will try to obfuscate or conceal the malicious documents – using techniques such as placing the document in a password protected zip file or embedding a malicious Excel document within a seemingly harmless Word document.

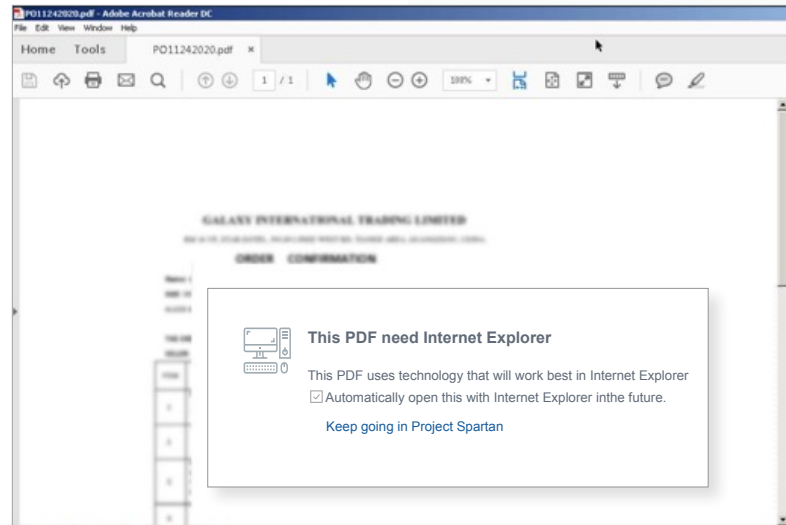
Some malware campaigns use malicious links within an otherwise harmless PDF, tricking users into downloading the malicious payload.

These links frequently use high-trust websites, such as file hosts like Google Drive, OneDrive, or Dropbox, to add the appearance of legitimacy.

All of these techniques are designed to manipulate users and evade email filters and sandboxes, which attempt to detect malware in transit.



**Figure 7** Example of a PDF document used in a Formbook malware campaign that contains links to malicious files

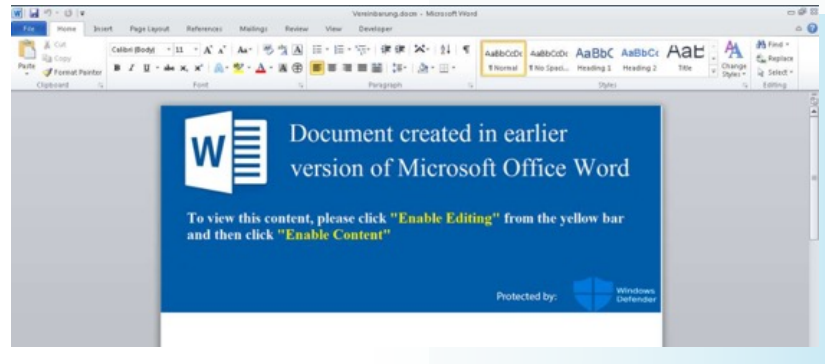


When looking at these common attack vectors, you might conclude that it is important to invest in best-of-breed email filtering and detection technologies.

However, while these are an important part of the security stack, they are only part of a broader solution and insufficient protection for the endpoints where the data lies. Email filters do not reduce the endpoint attack surface, which is ultimately where code executes, and data is stored.

Another challenge many organizations face is that employees may access personal email accounts, receive file attachments on social media, or may just download a malicious file by accident. **This underscores the need for reducing the endpoint attack surface through patching, privilege management, and application control** – which provide essential defenses against a wide range of attack vectors.

**Figure 8** Example of a Trickbot phishing document trying to socially engineer the end user into enabling macros



The primary social engineering tricks used to encourage users to enable editing and content (which, in turn, allows the attackers' malicious macro scripts to run) typically revolve around updates or security. Many users appreciate that updates, encryption, and security are important – so they willingly allow content to run, thinking they are helping improve security.

The example above shows how attackers use Windows Defender logos or other security tool names to create the appearance of legitimacy. While disabling macros is an option, many organizations require them for key business tasks, thus are unable to fully disable them enterprise-wide.



## Common Denominators

The everchanging phoenix-like nature of malware attacks makes today's threats more difficult for traditional AV solutions to detect and block. Most malware encountered in the BeyondTrust Labs has a unique file hash and is only used for a few hours before it is replaced by a new version.

Malware delivery techniques regularly change to evade email scanners, sandboxes, and automated analysis. Also consider that users may have access to personal webmail and other cloud services that could accidentally bypass organizational controls.


However, as we analyze the attack chains leveraged by these malware strains, we can identify common denominators. **When these common denominators are mapped onto the MITRE ATT&CK Enterprise Framework, we can classify the techniques found in our research and focus on mitigating underlying techniques.**

With this approach, we can proactively break the attack chain, rather than relying on the detection of a particular known bad file signature.

Regardless of whether it's a macro in a Word document, a zero-day exploit in Excel, or a drive-by download against Internet Explorer, we are seeing the same techniques being used by malware time and time again.



MITRE ATT&CK techniques provide a powerful way to break down attack chains, as well as building and evaluating defenses.



➤ However, a recent survey by MITRE found that, while **82% of respondents know about ATT&CK, only 8% regularly use it.**

[Industry Report: The State of MITRE ATT&CK® Threat-Informed Defense in 2021](#)

Of those who do use the framework, only 21% cite defensive analysis as the primary use case. This means that there is a huge opportunity to make better use of the framework to reduce the attack surface and prevent malware attacks.



## Most Common Techniques After Initial Malware Execution

### 35% T1047

Using Windows Management Instrumentation calls to launch a process out of the process hierarchy, typically PowerShell or Window Command Shell (CMD)

### 22% T1204.002

User Execution: Malicious File is opened, which then downloads and directly launches a malware executable

### 17% T1059.001

Launch PowerShell initially

### 15% T1059.003

Launch the Window Command Shell (CMD), used for initial execution

### 1% Other

Use other exploitable native applications, such as Rundll32, WScript, or Mshta

Thanks to the Emotet malware family, T1047 using Windows Management Instrumentation calls to launch a process is the most common technique used.

This technique is almost always used to launch PowerShell or CMD. As such, PowerShell (T1059.001) and the Windows Command Shell (T1059.003) continue to dominate as the primary and secondary execution techniques with attackers attempting to “live off the land” and avoid immediately dropping binaries to disk.



The number of malware strains that try to execute a custom executable payload directly from a user executed file T1204.002, such as a Word document, has been in steady decline for a few years. Today, this technique tends to be used only by less sophisticated malware.



➤ The general trend we are observing has been toward **using native tools to perform fileless attacks in the initial stages** until a strong foothold and persistence mechanism is established and security controls have been disabled.

Once this has been accomplished, the attacker may introduce their own custom executable to perform encryption or steal data.





## Trusted Application Protection Lab-Testing BeyondTrust Against Top Malware Strains

BeyondTrust's [Privilege Management for Windows](#) product is designed to eliminate unnecessary privileges, strictly control privileged access, and provide pragmatic application control to proactively reduce the attack surface.

Within this product is the unique [Trusted Application Protection \(TAP\)](#) feature, which provides an out-of-the-box policy designed to mitigate common attack techniques—including fileless threats—and prevent high risk applications, such as Web Browsers, PDF viewers, Outlook, and Microsoft Office from being exploited.

**To test the effectiveness of Trusted Application Protection, BeyondTrust Labs examined the attack chains of thousands of malware samples from the past year.** While malware will constantly change the content of the phishing emails, re-encoding payloads to evade AV, and use new scripting techniques to hide their intent, there is less variability in the attack chains used.

As an example, a threat actor might use a range of document types and create hundreds of variants with unique file signatures. However, every variant will launch CMD, then run a script that pulls down a custom executable payload and launches it. While the document changes, the script, the website hosting the executable, and the payload may all change—the attack chain remains consistent.

Trusted Application Protection uses both privilege management and application control capabilities to prevent these high-risk applications from launching custom malware payloads.

It also protects high-risk applications from more sophisticated DLL attack techniques, such as DLL injection, hijacking, and malicious DLL plugins.



For our analysis, we distilled 150 malware samples that represent the attack chains of some of the most prolific malware threats of 2020 – 2021.

As you might expect, the most successful malware families tend to vary their attack chains, resulting in a higher number of samples.

We then tested the samples against the Version 21.3 release of BeyondTrust Privilege Management for Windows with the default High Security TAP policy enabled on a fully patched Windows 10 system. This allowed us to evaluate the effectiveness of our solution against a representative set of malware attack chains.

Malware family	Total number of attack chain samples	Prevented by Privilege Management for Windows with TAP enabled	
Emotet	51	100%	✓
Trickbot	29	100%	✓
Loki	21	100%	✓
AgentTesla	19	100%	✓
NJRat	13	100%	✓
Formbook	6	100%	✓
Nanocore	4	100%	✓
Maze	3	100%	✓
Loader	2	100%	✓
MiniDuke	1	100%	✓
Cryptowall	1	100%	✓

*BeyondTrust Labs tested 150 strains against 58 MITRE ATT&CK Frameworks with BeyondTrust Privilege Management for Windows. Using patented Trusted Application Protection (a combination of Privilege Management and Pragmatic Application Control), with the proper configurations, policies, and settings, BeyondTrust Labs was able to disrupt all malware strains tested.*





While it would be foolish for any vendor to claim 100% security (although many do), our analysis found that **BeyondTrust Privilege Management for Windows is extraordinarily effective** at mitigating the techniques used by common malware threats over the last 12 months.

Through focus on reducing the attack surface and proactively mitigating the techniques, we can prevent a broad range of attacks without relying on file signatures or hashes.

**This means we can prevent the malware from succeeding by breaking the attack chain at the initial execution stage.**

Regardless of how many times the malware author changes the document or custom executable they drop to disk, Privilege Management for Windows can consistently disrupt the attack chain.

The next section of the report includes further insights into how common techniques are used, how they work, and how Privilege Management for Windows with Trusted Application Protection can prevent them.

## Diving Into MITRE ATT&CK Framework Definitions and Mitigations

### T1047 Windows Management Instrumentation (WMI)

One malware technique largely pioneered by Emotet was to launch a process using a WMI call. By applying this technique, the malware can evade common AV or application control blocks, where tools like PowerShell are prevented from executing as a child process of Word, Excel, or other commonly exploited applications.

Most malware will seek to execute a custom payload directly from the application used to gain initial access. As shown in Figure 9, the attacker has launched PowerShell directly from Word, making it easier to link the two processes together as part of an attack chain.

Emotet took a different approach. As shown in Figure 10, when the attack is launched there are no child processes associated with Word.

Instead, Emotet makes a WMI call to launch PowerShell. This causes PowerShell to launch as a child of WmiPrvSE. As shown in Figure 11, PowerShell is now disconnected from Word and blends in with other legitimate processes.

processp04.exe	SystemInternal Process...
WINWORD.EXE	Microsoft Word
powershell.exe	Windows PowerSh...
csrss.exe	Client Server Run...

**Figure 9** Attacker launches PowerShell from Word which appears as a child process under Word

processp04.exe	SystemInternal Process...
WINWORD.EXE	Microsoft Word
csrss.exe	Client Server Run...

**Figure 10** Emotet launches a payload, but it is not shown as a child process of Word

svchost.exe	Host Process for W...
WmiPrvSE.exe	WMI Provider Host
powershell.exe	Windows PowerSh...

**Figure 11** Using WMI, the payload appears as a child of WmiPrvSE and is not easily linked back to Word

While these actions represent legitimate functionality within Windows, they present a few challenges as the direct process relationship between Word and PowerShell (or any other malware payload) has been broken. Many security solutions rely on this relationship to track the attack chain. When security analysts look at the logs, there is often no clear link between the initial access (Word) and the payload script (PowerShell).

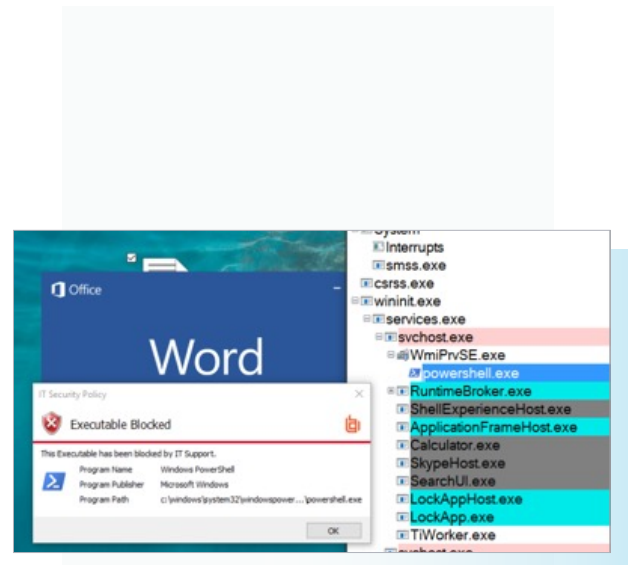
This combination of using PowerShell, a trusted Windows application, and WMI to sidestep process hierarchy is one of the reasons that Emotet became such a prevalent threat in 2020.

### T1047 Mitigations

MITRE recommends using Privileged Account Management and User Account Management to mitigate the risk of an attacker being able to use WMI with administrator privileges, both locally and across the wider network.

With Privilege Management for Windows, users start from a position of least privilege, automatically mitigating a substantive amount of risk. Trusted Application Protection within the product layers additional protection by leveraging the patented Advanced Parent Tracking capabilities to track and control processes launched using this WMI technique. This means that the product can link the execution of the payload back to a high-risk application and proactively block execution. Patents for these features include [US20190080081A1](#) and [GB2566347A](#).

The [Advanced Parent Tracking](#) feature is unique to BeyondTrust and provides multiple benefits beyond blocking malware. For instance, it also simplifies rule creation for allow lists or elevation rules where programs have a legitimate use for a COM or WMI call.



**Figure 12** Example of Emotet attack chain being blocked by Trusted Application Protection using Advanced Parent Tracking

As TAP is blocking the technique and breaking the attack chain—rather than detecting a specific payload—this represents a highly effective defensive approach against ever-changing malware files and scripts.

### T1204.002 User Execution: Malicious File

This is the classic case of tricking a user into opening a file by using social engineering techniques. The attacker then uses the file to launch an exploit or malicious macro to gain code execution.

**In 22% of cases, we observed attackers immediately downloading and launching a custom executable payload,** typically ransomware, for a short attack chain. While this is usually leveraged by the less sophisticated threat actors, it can still be very effective if the payload is not detected by AV or other security tools.

### T1204.002 Mitigations

MITRE recommends M1017 User Training and M1038 Execution Prevention. While user training is essential, most users can be tricked with targeted spear phishing, so it is imperative to both limit the privileges granted to users and to use application control for execution prevention.

Attackers often tailor malware payloads or files to look like legitimate applications (i.e. updates and installers). Robust application control can provide a safeguard by validating the publisher against an allow list. The user should also be operating in a least privilege environment to ensure that any malware cannot easily gain access to local privileges to disable security solutions or access the wider network.

Example of a basic attack chain using a malicious file (Word document)



Phishing Email



Word Document



ransomware.exe



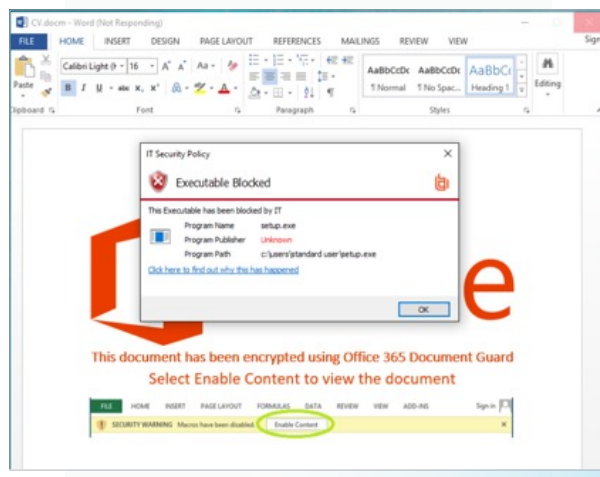
➤ BeyondTrust's Trusted Application Protection capability provides **out-of-the-box protection** for this technique by ensuring that “trusted applications” cannot launch a custom executable that has been dropped to the end user's workstation.

This protection is underpinned by the position of least privilege enforced by the BeyondTrust solution, which ensures the malware is unable to access admin privileges to drop their payload into a trusted location, such as the Windows System32 folder, or overwrite existing applications.

### T1059.001 – PowerShell used for Initial Execution

To evade detection, an attacker will use the powerful capabilities of PowerShell to profile the system, execute commands, and download payloads. Some malware strains, such as Trickbot, make extensive use of PowerShell scripts to disable security controls when the user has local admin rights.

There are numerous offensive tools written in PowerShell, such as Empire and PowerSploit, embraced by malware authors and red teamers alike. Since PowerShell is a legitimate Windows application, it is less likely to trigger a security alert than an unknown application that unexpectedly appears and executes.



**Figure 13** Malware payload blocked from launching by Trusted Application Protection

### T1059.001 Mitigations

MITRE advises on many possible mitigations, including M1049 Antimalware software, M1045 Enforcing Code Signing of allowed scripts, and M1042 Disabling and restricting features in PowerShell. These mitigations are all underpinned by M1026 Privileged Account Management.

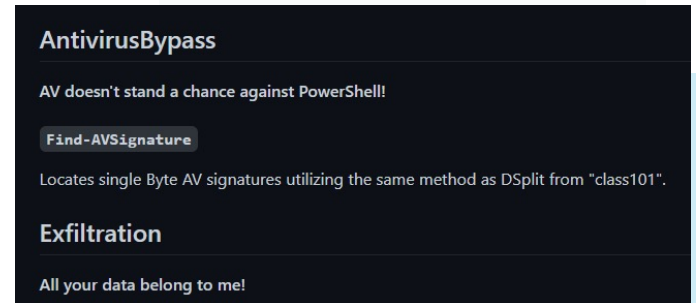
If the user has local admin rights, the malware can exploit those account privileges to disable the antimalware software and override any restrictions placed on PowerShell.

Privilege Management for Windows removes admin rights and provides a secure foundation on which to layer other security controls. BeyondTrust's product also provides Pragmatic Application Control, which enforces more granular controls on PowerShell to ensure that only approved tasks and scripts can be run.

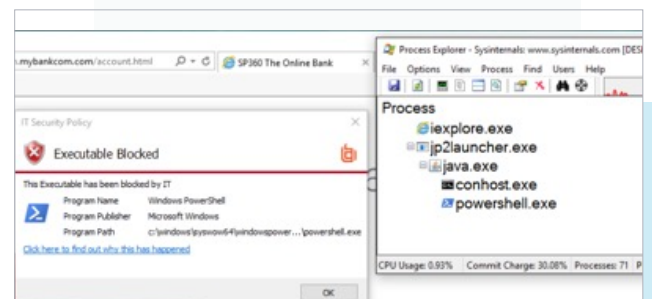
Trusted Application Protection (TAP) can automatically block high-risk applications from launching PowerShell. Because TAP can intelligently block based on the context, it can prevent malware from launching PowerShell, while still allowing legitimate use Powershell cases, if required. This approach delivers markedly enhanced security, while not interfering with user productivity.

### T1059.003 Windows Command Shell (CMD)

In a similar approach to the previous technique, attackers will attempt to use CMD to lie low, while executing scripts and commands. A good example of this is Trickbot, which will utilize obfuscated BAT script files for both execution and persistence using a scheduled task. When the BAT file is launched, CMD will interpret and execute the contents of the script, allowing the attack to gain execution without placing a customer executable on the system.



**Figure 14** Tools like PowerSploit offer the ability to bypass antivirus solutions using PowerShell



**Figure 15** Drive-by-download attempting to use a Java exploit to launch PowerShell block by TAP in BeyondTrust Privilege Management for Windows



The other advantage for the attacker is that CMD is usually allow-listed. Thus, it is not unusual for CMD to be seen running on a system. A user in a technical role may need to run CMD to perform a task, an installer or updater may use CMD, as well as a host of login scripts and ITSM products. With all these legitimate use cases for running CMD, the malware can blend in.

### T1059.003 Mitigations

MITRE advise M1038 Execution Prevention as the key mitigation for this technique. Although CMD is not as feature rich as PowerShell, it can still be used to inflict considerable damage, so limiting privileges is important.

Privilege Management for Windows provides ways to not only control the CMD application, but also to apply granular control over the execution of BAT or other script files. With these capabilities, organizations can adopt a secure least privilege stance without compromising on the end-user experience.

Trusted Application Protection automatically blocks high-risk applications from launching CMD directly or via a script dropped to disk in order to mitigate this malware technique.

### Other Techniques

We observed a small number of malware samples that attempted to exploit other native applications, such as Rundll32 or Mshta. Trusted Application Protection already blocks these applications from being launched by malware. As attackers seek out new native applications to exploit, BeyondTrust Labs continues to monitor for emerging attack techniques that can be prevented using TAP.

Additionally, Trusted Application Protection is also able to track application execution across multiple processes in a hierarchy, allowing it to block payloads and exploit native tools at multiple points in the attack chain for maximum protection.

With these capabilities, organizations can adopt a secure least privilege stance without compromising on the end-user experience.



## 5 Critical Steps to Complete Endpoint Security



➤ According to IDC, **70% of successful breaches start at the endpoint**, while Ponemon estimates 60% of attacks are missed by antivirus software.

In our analysis of 150 common malware threats that have plagued businesses around the globe for the past year, we have clearly demonstrated the remarkable effectiveness of Endpoint Privilege Management solutions, such as BeyondTrust Privilege Management for Windows & Mac and Privilege Management for Unix & Linux products, in proactively stopping these and potential future threats that leverage similar attack chains.

Yet, no one solution can be the sole basis for a strong endpoint security strategy—it takes an ecosystem of solutions working in tandem.

All too often, malware will not only use multiple techniques to evade detection, but will also exploit excessive privilege granted to end users to disable security controls, which completely undermines your defenses and security investment.





Malware threats can seem overwhelming, with thousands of variants appearing every day and a constant stream of zero-day threats and emergency patches.

However, if we look at the heart of every attack, there are some fundamental tactics that we can address:

### Execution and Persistence

An attacker needs code to execute; if you have control over what can execute through allow listing, you limit the attacker's ability to succeed.

### Privilege Escalation

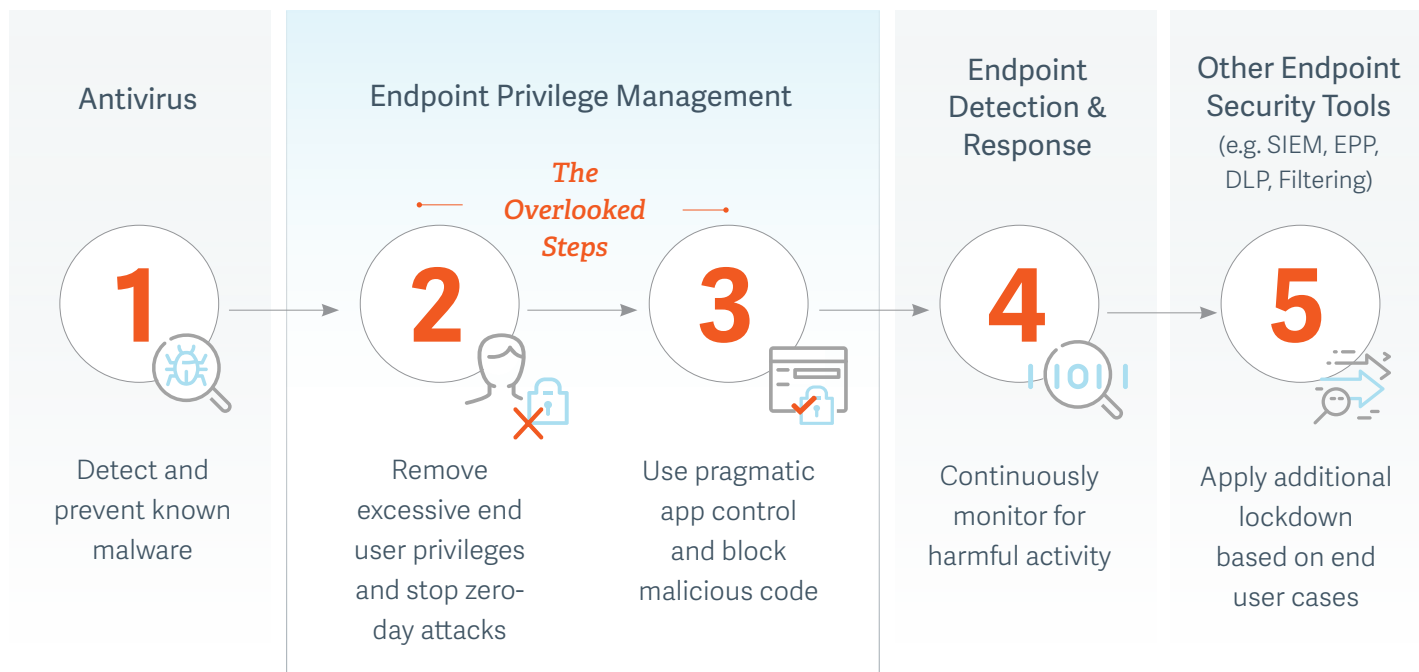
Without access to a local administrator or other privileged accounts, the attacker is limited in the systems and data they can access.


### Defensive Evasion

To evade detection, an attacker needs both the privileges and the ability to execute code to tamper with system settings and security tools.

There are five critical components of a holistic endpoint security strategy built to withstand today's threats landscape, while also enabling organizations to confidently advance along their digital transformation journeys.

## The 5 Critical Steps to Complete Endpoint Security





Endpoint privilege management is key to **preventing and mitigating endpoint attacks**, while technologies such as endpoint detection and response (EDR), play important roles in detecting and analyzing threats.

Combining these technologies as shown in the “5 Critical Steps to Complete Endpoint Security” on the previous page, delivers powerful synergies.

For instance, by implementing endpoint privilege management with application control, you not only benefit from its essential security capabilities, but also optimize performance of other endpoint technologies, such as EDR, by preventing zero-day attacks, reducing the noise.

This report highlighted how several key factors over the past year have substantially increased the security risk of many organizations, and also shed light on how threat actors have responded with an increase in malware threats using local admin rights to disable security controls, steal credentials, and move laterally.

**These risks are entirely possible to mitigate with the 5 steps approach.**

“Removing admin rights from end users is one of the single most effective ways to improve overall security posture, and more granular privilege management can achieve this goal without impacting productivity.”

— Dan Blum,  
Cybersecurity Strategist



## > Schedule a Demo of Privilege Management for Windows

Visit our website at [beyondtrust.com](https://beyondtrust.com).

## > Additional Resources

BLOG	<a href="#">How to Protect against EMOTET - "The World's Most Dangerous Malware"</a>
WHITEPAPER	<a href="#">5 Critical Steps to Complete Endpoint Security</a>
WHITEPAPER	<a href="#">2021 Microsoft Vulnerabilities Report</a>
ANALYST RESEARCH	<a href="#">KuppingerCole Executive Review: BeyondTrust Endpoint Privilege Management</a>
ANALYST RESEARCH	<a href="#">2021 Gartner Magic Quadrant for Privileged Access Management</a>



BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

[beyondtrust.com](https://beyondtrust.com)

V2021\_08\_ENG



## APPENDIX: THREAT SAMPLES TESTED

Trickbot	Word	4faf7bbebcbceb84a20d23c76a000bfb
Trickbot	Word	6699fdf727451b58e3071957364fb5c4
Trickbot	Word	7ea1831e71c8e0030a4c5e89b21d61bd
Trickbot	Excel	fb7103737708c995ca3610991cd153b4
Trickbot	Excel	1e61503a771fb63d299ee9ce416f5a35
Trickbot	Excel	10f8bac6c273c1d96bbaecf6eeb60b62
Trickbot	Excel	10e409342fe369c34f329831646816a1
Trickbot	Word	ccce712fa29d5bd166f8a38b17550c4a
Trickbot	Word	6054da9bf92baed888d7c0bf9b608859
Trickbot	Word	4f658a33fe28c0c78f92db779f0aba30
Trickbot	Word	28ebf979ca74ac6a98be6b5f36134b44
Trickbot	Word	48e38c6ace1d943214e3efe7a5a1af3d
Trickbot	Word	da170c9ea70d60d7a240ecaa38ed3cc1
Trickbot	Word	a3cb2e0b06d010991dc487c596bdd109
Trickbot	Word	13b34b67a0180ae27e0c64a0bcac4b08
Trickbot	Word	cc242a96f5b9991c5e636f1f8d73303b
Trickbot	Word	009abd2dc7cf65b3040dbec822ebbbe6
Trickbot	Word	1da58468ee0c30b6f7647827df1f783c
Trickbot	Word	3a780caaf158a2f8c285b517669b94d4
Trickbot	Word	96729fda35f2ef7f135f6963e018b1a5
Trickbot	Word	eafd7f3aaa046c7f885159b7c724a48e
Trickbot	Word	a4c2872ab1cc6987700f8a6407a37947
Trickbot	Word	cc90b28cb8401de8a215dedc894286f4
Trickbot	Word	42c7039020541a83aa0122c20bce11af
Trickbot	Word	36beeb861147eadf57a6c2da15917f84
Trickbot	Word	ce26036f24bac65b3bc1da308423aeb7
Trickbot	Word	cbe4251e4eac6bef33a519a8dc14cc5d
Trickbot	Word	7f52cedfa9542805b974a265e3ac6f50
Trickbot	Word	1f388f42eb89dda6fcf4c9ed566237ec
AgentTesla	Excel	949f8f0559b9aa9c2af61f0f061ff7cf
AgentTesla	PowerPoint	9bdc3104c189660f2e9e4b72307baea3
AgentTesla	PowerPoint	9bdc3104c189660f2e9e4b72307baea3
AgentTesla	PowerPoint	5c63ab7763e609cf490333be0be26596
AgentTesla	PowerPoint	00cc498ab93d8815036efdbb4239edc8
AgentTesla	Word	a067f380a1b8d508bd6f8a934a0aefb9
AgentTesla	Excel	b9f34ad3d91caed2e75accd61830922f
AgentTesla	Excel	47ba7c126c69593c032b01e46046d795
AgentTesla	Excel	770fac8452fb226f8c2c678898368806
AgentTesla	Excel	b0100a80c042c9efe7a8ca303599f29e
AgentTesla	Excel	ae532c0452bbe4d93a4793d00c5aab82
AgentTesla	Word	8c894add6233af16143b2b8244c72a79
AgentTesla	Excel	354c0f7c3c824b699a310afdd96a7a29
AgentTesla	Excel	47ba7c126c69593c032b01e46046d795
AgentTesla	Excel	7330db045ca2cc98a46e37a3841535f9
AgentTesla	Excel	7d1347b165972290cace9e640fc430e7
AgentTesla	Excel	045643593bac051413f884cdc2c327b9
AgentTesla	Excel	0fa1f0ea9085f62e485d296e37d3fe11
AgentTesla	Excel	844c62e35732eb33612cec153258dbfb
Loki	Word	7e39c872a6b098f0cc57f9f39890968b
Loki	Word	f6e621987066e44d55694457706f5bec
Loki	Excel	088e511c9db176227c25ecd238984638



Loki	Excel	669e6674d078745635c166249995cb40
Loki	Excel	2cf27f932ba0c8eb8f9686cfeb56e1ae
Loki	PowerPoint	89ddfb9ac3039654002e21643d1a1f9
Loki	Word	541d7f143e1ea710ce7a0a4bd8b13f07
Loki	Word	16169b24b5781b141ead622fd34e2cb7
Loki	Word	fd2e98ae762daaa9b265a4f717f19495
Loki	Excel	889ff85370bb381d66ad68c474f9dfcb
Loki	Word	579d426d8704607984cbe9af5987aa8e
Loki	Word	f5a14fde55f0b67553971a7634a215bd
Loki	Excel	572101b633037231e9844826037b6bff
Loki	Word	b13937732c5e2705f255e67571bae2a1
Loki	Excel	2b692512bc2f32f8956a73675e035e96
Loki	Word	a6c1203bed1ceeb336e6a2fce5973f5e
Loki	Word	a998058805323bcd389a1e37f5b9138f
Loki	Word	c263c49996b72c8c433088bf4316a914
Loki	Word	bc076fa757ce94bce55767ca6f6a1958
Loki	Word	6f220124e19c74cd4963ad1330e0e5c6
Loki	Word	a25bd34a59c15c3b5c69463f22145f62
Maze	Word	1304606861c8d05f5bba92d225adc69a
Maze	Word	49b28f16ba496b57518005c813640eeb
Maze	Word	1a26c9b6ba40e4e3c3dce12de266ae10
NJRat	Word	4e8e44236943452997311a750da96dc9
NJRat	Excel	b9392f059e00742a5b3f796385f1ec3d
NJRat	Excel	e4a3af5634ecbec98b170dd76987b5aa
NJRat	Word	4e8e44236943452997311a750da96dc9
NJRat	PowerPoint	a6058257767a279c9a22dd1a6391c389
NJRat	Excel	2b21b35b388cf7cf2f36a914f69c6fff
NJRat	Excel	f1fa05dd08ab91058c98da0f52306867
NJRat	Excel	0c3f8edc8224fb687951bd5436c5532f
Nanocore	Excel	aac525d2a3f9c97d9c75c2b6ecd5ef7d
Nanocore	Word	d521cb1040f08b07e4dbaf48d946eaea
Nanocore	Excel	24924c11572af929002ca044254020b4
Nanocore	Excel	06b1844dd4e364248441ef471d4ef92e
Emotet	Word	d743137a26f7a7bfa83790b06e387c48
Emotet	Word	98c46848a412d7ae831ce4cfd1e453f
Emotet	Word	607ff85495cbe04824cb2527b1567d6f
Emotet	Word	bd7f1c8c555ce80c9a7356877c8602ef
Emotet	Word	0eb2b3e34f5387f682ea5f2813f64a7c
Emotet	Word	0cc322b45bb881869b71e3b98158f519
Emotet	Word	ceb1aa4b977b01cf2c56bbf2a39f7268
Emotet	Word	69f2aa8e265b0a19c125471c5c43ef0e
Emotet	Word	ed97c23ae28330668ac7857640f8e9d1
Emotet	Word	a8f422b7984dbf5a66fe95256591f7e3
Emotet	Word	a9cc1e15d6df7fb6261ff215dd332464
Emotet	Word	7112d68dba3ee9be9e171f9fc193d69e
Emotet	Word	8f25f1c09b9556a7df3a7e09e7b9a7bf
Emotet	Word	26646a14cd7b48eb5ce2174f136c0cd6
Emotet	Word	429fe2a3470f72b737806f4baf857c95
Loader	Excel	af68a5c2b36866230898d45574fd8935
MiniDuke	Word	f27ffc3d3ff7a2ddc6728d9495427ee5
Loader	Excel	f27ffc3d3ff7a2ddc6728d9495427ee5
Emotet	Word	223975e6f03f5cc32074a00e82f8cf99



Emotet	Word	d7e6921bfd008f707ba52dee374ff3db
Emotet	Word	bacb48f9663397f321734008ac75fcd8
Emotet	Word	c50a5a5166c9353811c3c6262daf44c8
Emotet	Word	a2f6ed15e827ec2c068ad6aaca80b893
Emotet	Word	1027ef800be863cd85e4731052935b25
Emotet	Word	1a72a81deb26a42da101cca7837afe21
Emotet	Word	593d2208d4b6f24573ef1d7a16cdeb6c8
Formbook	Excel	db6fdb35327cfe36f818f220818fc03
Formbook	Excel	6d87c00c8562c1671f9d8f293e524f0e
Formbook	Word	5c2a6d7c703571d4f8b2ead028dd5fa9
Formbook	Excel	ccaacde2a2fea467aacb4d46c0f6d92a
Formbook	PDF	7992642289408bf47ff691a1265e1cb7
Formbook	PDF	b6631eed423720a3cda49644530cc04
Emotet	PDF	cf8829b6a96adf5ff4d116069df946f6
Emotet	PDF	180cbb4bbae718694c0fd1c56b1ba0e6
Emotet	PDF	ecfdb5763ad559b7f62857dd61cf7461
Emotet	PDF	241f0996e352b4f48403e41c1b8965d43
Emotet	Word	d0a13c59278e12805678398ec844c264
Emotet	Word	fa9d1eae727d2a3da63392214d12f92c
Cryptowall	Word	54bd0ee44c394b526fb57b10fd20a407
Emotet	Word	fa5eef4f9ca20cc1a937f91aa8fb92f0
Emotet	Word	7258d39f41a2bbf908aa0da116d71785
Emotet	Word	27e3a6a2a661389c26f2ca9cbf39cc0f
Emotet	Word	13b9d586bb973ac14bfa24e4ae7b24f1
Emotet	Word	f8f9e046a1c0440d4670efc165a3ccb3
Emotet	Word	1a72a81deb26a42da101cca7837afe21
Emotet	Word	30e0ed6edf9874c15a0e38f53fac2921
Emotet	Word	3e920f73bd01f7f2bc523365586cb1a6
Emotet	Word	ff29b4ff041b8b04fbf51e5059c823d3
Emotet	Word	992e1be2c96fd2b848f0fd718e5f3466
Emotet	Word	4aaa2599e6477717c623d0a7b0ee4b50
Emotet	Word	e5f1c07d8ef2670f9cfb6ce9441a7343
Emotet	Word	2fd21fd4e4418e6e0ad1084479b3e496
Emotet	Word	a4cb587df39fbf9307d8639d3496b921
Emotet	Word	f1228af237341638ae0973e44f78d4f6
Emotet	Word	1c666e1a9958ad00a433fe9186df68fa
Emotet	Word	3182a6576e47b1922f12c85c7e19c373
Emotet	Word	396fed694f205dbbe239bdc6d15a17db
Emotet	Word	d904dcff569da842a2774940ba27d4ef
Emotet	Word	3101205da4418f5932b20d33ba0c8de6
NJRat	PowerPoint	ceb3a5a3ba16fd2aa2098bc1b9250df6
NJRat	Word	2cc1095aabe78d0b38caad040ef1a215
NJRat	Word	4e8e44236943452997311a750da96dc9
NJRat	Excel	2b21b35b388cf7cf2f36a914f69c6fff
NJRat	Excel	bac74e3006b9c6d544d2ace87a23ac40