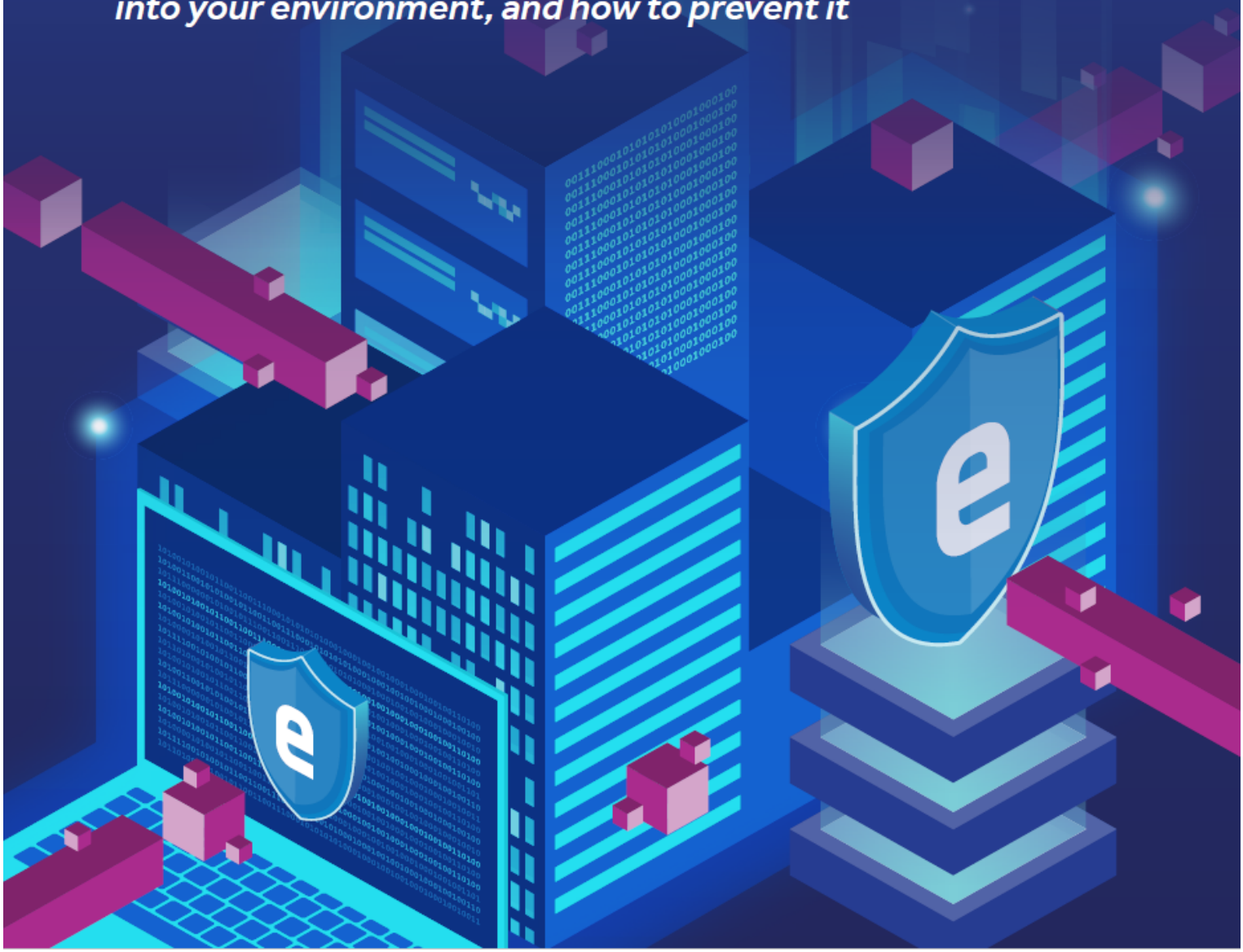
ITSpecialist eSENTIRE

RANSOMWARE REPORT

Disrupting Initial Access

An examination of how malware gets into your environment, and how to prevent it



Introduction

Ransomware has become a topic of discussion in executive suites around the world as cybersecurity leaders grapple with the magnitude and impact of this risk. Successful attacks unfold in mere hours from Initial Access to data exfiltration and deployment of ransomware, causing CISOs to re-evaluate their cybersecurity program, posture, and controls. Similarly, Security Operations teams also need up-to-the-minute threat detection capabilities and response playbooks to fully respond to and remediate these attacks.

In the past year, we have seen notorious ransomware gangs such as Conti[1], Lockbit 2.0, Hive, and BlackCat (ALPHV) run sophisticated operations to deploy ransomware for maximum disruption, exfiltrate sensitive data, and employ advanced extortion tactics to demand the highest ransom payments possible.

In many cases, these gangs operate as businesses with revenue models that include exchanging accesses to disabled systems and promises not to release stolen data (i.e., double extortion) for cryptocurrency. However, before they can fulfill these objectives, they must gain entry ("Initial Access") into your environment.[2]

Over the years, ransomware gangs have developed an arsenal of tactics, techniques, and procedures (TTPs) that make it possible for them to progress from a single compromised endpoint to a widespread intrusion in a matter of minutes.

In February 2022, eSentire's Threat Response Unit (TRU) team investigated an incident involving the IcedID malware.[3] In this attack, it took less than 20 minutes from the time a user opened a malicious email attachment containing IcedID to the deployment and execution of the Cobalt Strike stager.[4] We see hundreds of incidents of this nature each year as threat actors attempt to break through the preventative measures put in place by the security leaders across our global customer base.

This report summarizes the ever-changing TTPs leveraged to achieve Initial Access from security incidents thwarted by eSentire's 24/7 SOC Analysts over a two-year period between April 2020 to April 2022. Experts from our TRU team have summarized an analysis of Initial Access trends and presented recommendations on how your organization can prevent attackers from establishing initial footholds and deploying malware.

Modern ransomware is unpredictable given the interconnected nature of these groups and multitude of ways they can gain access to target networks. While not every threat or technique mentioned is directly associated to ransomware, increasing your resilience to these initial access threats will limit your exposure to follow-on attacks including ransomware.

Disrupting Initial Access

In recent years, a robust ransomware-as-a-service ecosystem has developed in which specialized cybercrime gangs perform different stages of an attack. Groups that provide Initial Access as a service execute orchestrated campaigns and automated attacks to break into your IT environment, establish a persistent presence, and perform reconnaissance. Then, using the intelligence gathered, they calculate a market value for the access and sell it on a cybercrime marketplace. Any threat actor can purchase this access to deploy ransomware or pursue other objectives.[5]

Although vertically integrated ransomware gangs may perform most, or all, of the operation alone, they typically have different specialized departments for each stage of the cyberattack. In essence, these ransomware gangs resemble enterprise organizations.

In general, the Initial Access TTPs tend to be highly automated (left side of Figure 1), while the subsequent intrusion actions are more manual (right side of Figure 1).

What's more, the early stages are also where threat actors invest enormous effort on innovation and real-world experimentation with a particular focus on defeating reputation filters and perimeter protections.

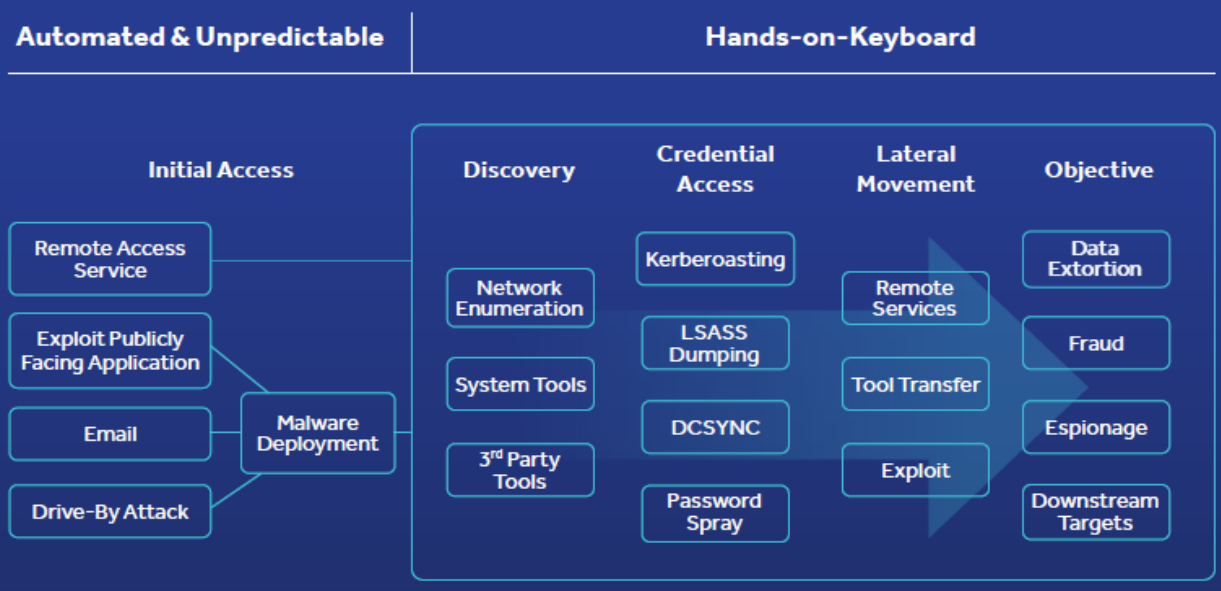


Figure 1—High-level view of common attack paths

Observations from eSentire's TRU reveal that the TTPs used in later stages of intrusions don't change as rapidly as those used to gain initial access. For example, an attacker may package their malware in a new way to evade filtering, but once executed, the malware's behavior is likely to be very similar to past incidents.

While the mid-to-late stage intrusion TTPs may be somewhat familiar, that doesn't mean detecting them is easy—or even comparatively easier than detecting the Initial Access TTPs. Attackers often leverage the same built-in system functions that administrators use, and it's only by correlating multiple sources of telemetry that malicious intent can be identified. Once an attack transitions from automated to manual (or interactive), threat response becomes more complex—and more costly.

This is largely due to the scope of the response capabilities expanding significantly (e.g., multiple compromised endpoints/accounts) and the attackers' resilience (e.g., multiple backdoors and other persistence mechanisms). In addition, a skilled adversary can actively react to your security team's countermeasures and switch tactics, drawing out the attack.

Defend Your Organization Against Modern Ransomware

Although identifying and containing threats during the early stage of an attack is ideal, this is precisely where threat actors appear to focus the bulk of their innovation efforts. How you respond in these situations – with speed, coverage, and expertise – is critical. You need a Managed Detection and Response (MDR) provider acting as an extension of your team that can go head-to-head with the toughest adversaries to defend your organization from a crippling cyberattack.

The SunWalker incident exemplifies a modern ransomware attack scenario that combined multiple tools and techniques, including an 8-hour long hands-on-keyboard cyber combat between a threat actor and eSentire's team of Elite Threat Hunters.

In this report, we examine the evolution of ransomware and outline the SunWalker attack in detail to demonstrate how you can prepare and execute an effective multi-layer defense that combines people, process, and technology against modern ransomware.

Download the report

High-level Trends in Malcode Delivery

Despite the attention given to remote exploits, most security incidents still rely on humans unwittingly aiding the attacker, usually by executing malicious code ("malcode"). Unfortunately, executing malicious script files and shortcuts is as simple as double-clicking.

For attackers, the question then becomes: "How can users be enticed into clicking on something they shouldn't?"

Figure 3 shows the year-over-year trends in malcode delivery mechanisms spanning 2020-2022, as determined by TRU:

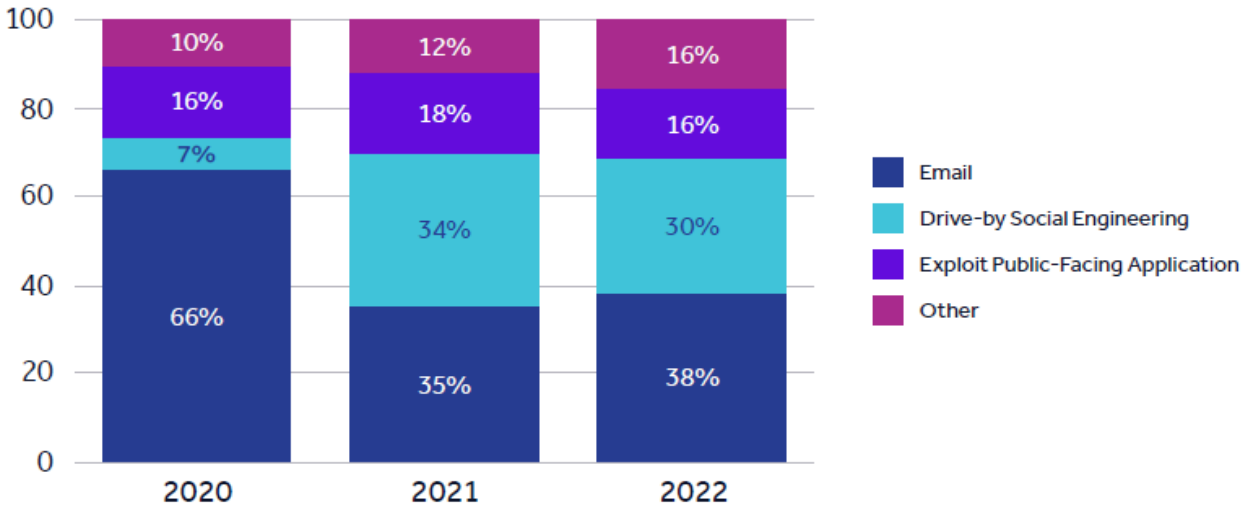


Figure 3—Year-over-year trends in malcode delivery, 2020 through 2022

Over the three years, the portion of incidents attributed to exploiting public-facing applications has remained relatively constant. There has been a small 5% increase in threat actors leveraging attack vectors such as abusing trusted relationships, drive-by exploitation, remote access services, supply chain compromise, and insider threats (denoted as "Other" in Figure 3) to gain Initial Access.[6]

The most significant changes are shown in the use of email vs. drive-by social engineering:

- **2020:** Email dominated as the delivery vector, accounting for 66% of incidents. The malicious code itself often took the form of macros embedded within Microsoft Word and Excel files. Only 7% of all malcode was delivered via drive-by social engineering.
- **2021:** There was a surge in drive-by social engineering tactics. This shift was likely driven by hardened defenses that made bypassing email controls more difficult as well as the implementation of phishing and security awareness training. The strategy proved so successful that the use of email as the delivery vector was nearly halved (35%) while drive-by social engineering surged to 34% (from 7% in 2020).
- **Year to Date Through April 2022:** Email-borne malcode has shown a slight resurgence (38%), with HTML smuggling and ISO shortcut attacks emerging as alternatives to macro-based execution. Drive-by social engineering has decreased slightly (30%) as a result, but whether these proportions will remain consistent through to the end of the year remains to be seen.

The subsections below will briefly examine the three most common malcode delivery mechanisms.

Email

Email is highly monitored and less likely to succeed against moderately hardened targets. Any malcode relying on email as the delivery vector must defeat company-wide policies such as email filtering, anti-malware, and endpoint mitigations including macro controls. Even if the malcode successfully gets through, users still need to be convinced to perform an action (e.g., enabling macros) to execute the malcode.

However, soft targets can be compromised easily, and adversaries can use tactics like business email compromise or thread hijacking to bypass the reputation filters guarding more sophisticated, higher-value targets.

Figure 4 demonstrates a six-month snapshot of specific email-borne threats observed by TRU. The data shows that Emotet has experienced a resurgence [7], while other malware families like SquirrelWaffle[8], Qakbot, AsyncRAT[9], and IcedID have also enjoyed considerable success.

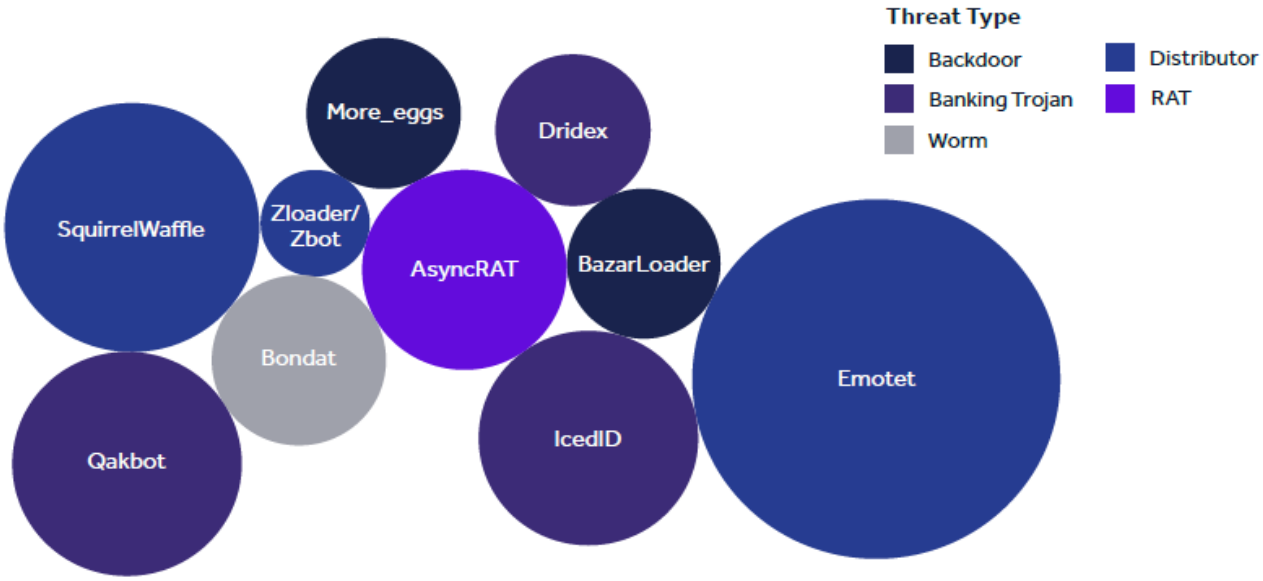


Figure 4—Six-month snapshot of email attacks that successfully bypassed defenses

Although simple attacks that abuse Windows features continue to be the norm (Figure 5), these attacks can be eliminated by unregistering ISO files, blocking abused filetypes at email gateways and increasing user awareness of the risks associated with opening attachments.

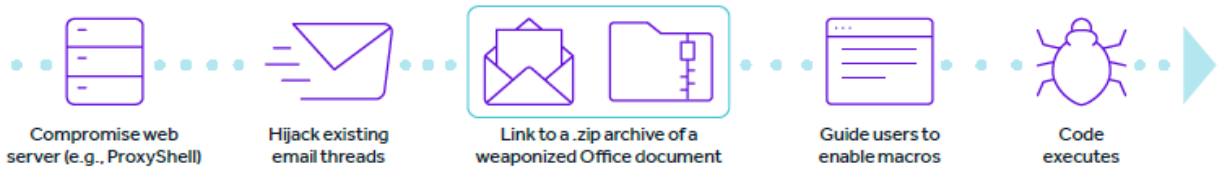


Figure 5—A common SquirrelWaffle attack flow combines thread hijacking with malicious macros

Drive-by social engineering

Drive-by social engineering attacks are simple, but effective, and rely upon manipulating the victim into downloading, and opening, malicious files from web browsing sessions. These files are typically disguised as legitimate software or documents. Broadly speaking, attackers lure victims by poisoning search results (using a technique known as SEO poisoning) or by injecting fake warnings for out-of-date software into browsing sessions.

Figure 6 demonstrates the specific threats observed by TRU that leverage drive-by social engineering tactics to lure victims into executing malicious code and gaining Initial Access into their company's environment.

Although these attacks have always existed, threats like Socgholish, Gootkit Loader, and SolarMarker find success by taking advantage of cloud services to hosting website landing pages and bypassing reputation filters.

As with email-borne malware, these attacks are enabled by default behaviors found in operating systems (e.g., executing a script file by double-clicking on it). Until that behavior changes, we will continue to see adversaries explore and leverage these attack vectors.

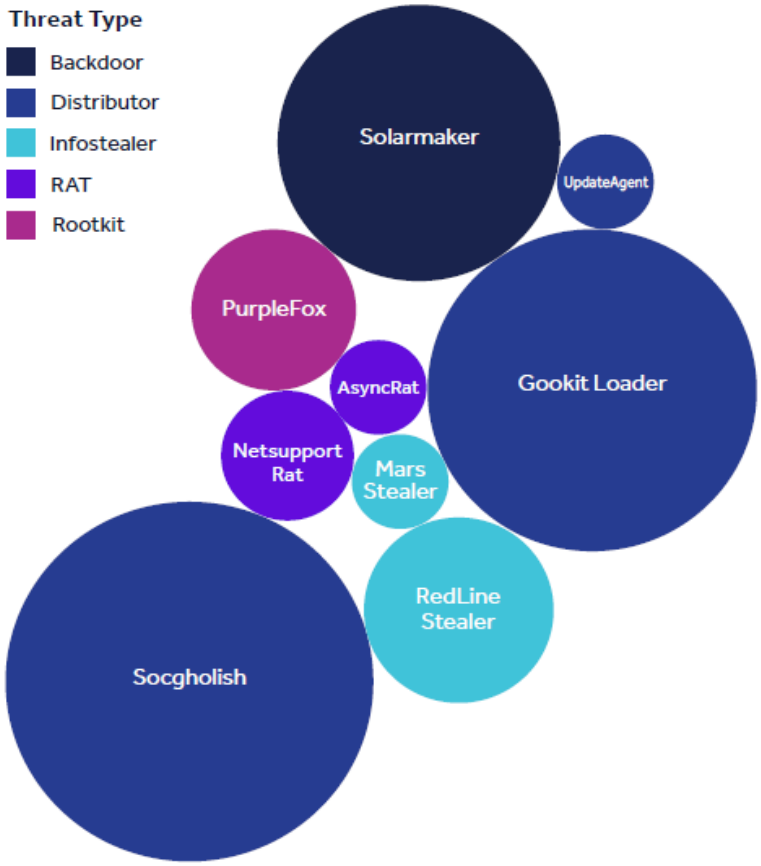


Figure 6—Six-month snapshot of drive-by social engineering attacks that successfully bypassed defenses

Figure 7 demonstrates a common attack workflow used by threat actors to execute SolarMarker[10] and Gootkit[11], in which the threat actor disguises a malicious file as a template or another document likely to be searched by a target demographic (e.g., "aviation safety agreement" or "new patient intake form").

The document is hosted on a compromised website or a front site, which itself is hosted in the cloud, and SEO poisoning techniques are used to rank the malicious websites higher on search engine results. The user, who has no reason to suspect that the file (or the website itself) is malicious, downloads it and, upon opening it, unwittingly executes malicious code.

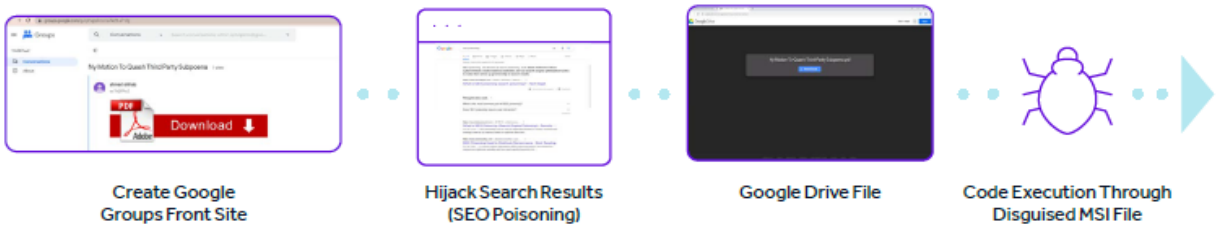


Figure 7—A common SolarMarker attack path leverages drive-by social engineering

On the other hand, Socgholish continues to have success using scareware tactics, usually masquerading as a fake update for web browsers to trick users into running malicious scripts or executables.

Exploit public-facing applications

Threat actors will also exploit software vulnerabilities to achieve a range of malicious purposes. When an application or service is public-facing, that purpose is often to achieve Initial Access. Unlike the email and drive-by social engineering vectors, remote exploits don't depend upon a user unknowingly enabling the attack.

Additionally, there are a wide array of tools that make it easy for threat actors to find and exploit vulnerabilities, which is one reason why remote exploitation has remained a constant threat in recent years. In fact, through the first four months of 2022, the Apache Log4j vulnerability (specifically CVE-2021-44228) accounted for the most remote exploits encountered in eSentire's threat investigations.

Unfortunately, the reality is that attackers are often presented with plenty of opportunity because today's IT environments are extraordinarily complex and patch management remains a tedious, operationally intensive activity. This is prime reason why every organization should engage a Managed Vulnerability Services (MVS) provider to help their security teams identify vulnerabilities continuously, prioritize remediation against the greatest potential business risk, and reduce operational, staffing, and resource constraints.

Recommendations to Manage Initial Access Risks and Prevent Ransomware

Email-borne threats, drive-by social engineering, and remote exploits are collectively responsible for driving Initial Access in **more than 84%** of the incidents investigated by TRU through the first four months of 2022.

Therefore, you can meaningfully reduce your organization's risk of ransomware and other malware by hardening cyber defenses against these three vectors.

Combating email and drive-by social engineering

The first line of defense against attacks that exploit user behavior is Phishing and Security Awareness Training (PSAT). An effective PSAT program emphasizes building cyber resilience by increasing risk awareness, rather than trying to turn everyone into security experts.

To that end, look for a program that:

- Drives security awareness and behavioral change with user-specific training to reduce the risk of phishing-based intrusions
- Measures user resiliency by testing the user's ability to identify and avoid the latest phishing tactics and campaigns
- Identifies and tracks improvement by identifying the high-risk users and groups on your team to reduce the risk associated with their privileges and access
- Alleviates resource constraints by automating testing and training, reducing the burden on your team
- Meets regulatory requirements by helping your security team comply with state, industry, & professional regulators and other obligations.

An eSentire-backed survey of experienced penetration testers showed that 99% employ social engineering—with 39% indicating that phishing is the technique most likely to succeed.

Learn more about:

- What to look for in a PSAT program
- Measuring the success of your PSAT program
- Why so many PSAT programs fail

While a security-aware workforce contributes to a strong cybersecurity posture, you should also implement controls focused on common code execution techniques. For example, the default in Windows is to execute script files when double-clicked. The risk of a user unwittingly aiding an attack is increased when file extensions associated with scripts are hidden from view for aesthetic purposes.

To manage common code execution risks, we recommend that your security team enable policies that:

- Always display file extensions for known file types
- Use Windows Attack Surface Reduction rules to block JavaScript and VBScript from launching downloaded content[12]
- Employ an Endpoint Detection and Response (EDR) tool to detect and isolate threats before they spread laterally[13]

Combating remote exploitation of public-facing applications

In the last few years, enterprise IT environments have transformed significantly. On-premises applications and services have moved to the cloud, IT and OT (Operational Technology) have intersected, the Industrial Internet of Things (IIoT) has arrived; and laptops and mobile devices have replaced dedicated workstations. Lurking in the background, shadow IT (systems that are in use but aren't officially sanctioned) is an ever-present risk factor.

Unfortunately, the harsh reality for every business, including yours, is that you can't protect against what you can't see. Therefore, securing against remote exploitation attempts requires a comprehensive vulnerability management program that combines three elements:

- Continuous awareness of the threat landscape (e.g., threat advisories, cyber news, etc.)
- Disciplined, risk-based patch management
- Vulnerability scanning to understand which systems are inadvertently exposed

While each element is vital, vulnerability scanning is especially important. By employing automated reconnaissance techniques, vulnerability scanning continuously provides full visibility and contextual awareness across your attack surface, alerting you to risks and helping direct cybersecurity efforts.

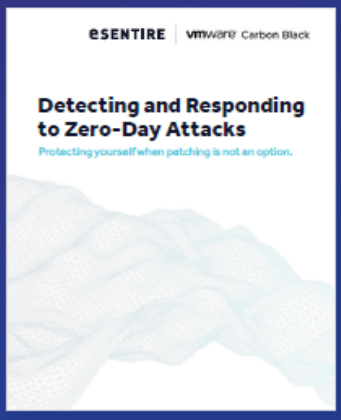
An effective **Managed Vulnerability Services** program will:

- Keep up with your attack surface (e.g., mobile devices, OT, IoT, virtual machines, and cloud environments)
- Dynamically incorporate the latest CVEs and zero-days
- Prioritize remediation against greatest potential business risk
- Track and measure programmatic improvements
- Reduce your operational, staffing, and resource constraints
- Satisfy your regulatory requirements

A zero-day attack is an attack that exploits a software vulnerability that is not known to the vendor or its users. Because the vulnerability is not known to the vendor, there is no patch to repair it.

And unfortunately, zero-day attacks are on the rise.

However, while the zero-day exploitations themselves cannot be prevented until technical details are known, it is often possible to detect post-exploitation activities through advanced behavioral analysis and other techniques.



Download the report

Proactively combating ransomware using MDR + IR

As large-scale, high-profile cyberattacks continue to make headlines, there's growing awareness among key business stakeholders that cyber defenses can, and will, fail. As a result, today's CISOs should adopt an "assume breached" mentality and create a proactive cybersecurity strategy to respond to, and remediate, cyber threats.

Small and mid-sized organizations rarely have the resources to build, staff, and maintain an in-house 24/7 SOC. This is a time-consuming, labor-intensive process that can cost millions of dollars a year. Adding to the challenge of building a strong security operation is the increasing sophistication of present-day threats, the complexity of modern IT ecosystems, and the need to secure remote and hybrid workforces.

Herein lies the need for real **Managed Detection and Response (MDR)**.

You need to rely on a trusted partner that can provide robust 24/7 security monitoring capabilities so you can put your business ahead of disruption. When you engage a quality MDR provider, you benefit from:

- ✔ Complete visibility and coverage across your attack surface as a result of multi-signal ingestion, enabling deeper correlation and threat investigation capabilities
- ✔ High fidelity detection and automated real-time threat disruption driven by an AI and ML-powered XDR platform to stay ahead of new and emerging cyber threats
- ✔ Continuous protection by a team of 24/7 SOC Analysts and Elite Threat Hunters who rapidly investigate, contain, and shut down threats when an automated response isn't possible
- ✔ Original threat intelligence driven by a team of world class threat researchers who actively hunt the most advanced undetected threats and deliver original research, curate threat intelligence, and build new detection models
- ✔ Reduction in cyber risk over time as the detection models will be mapped to industry standard frameworks like the MITRE ATT&CK, which can then be leveraged to quantify your organizational cyber risks and inform the overall cybersecurity strategy

In today's world, your team needs what MDR delivers – the capacity to perform rapid threat containment and remediation when an incident occurs. However, in the event of a successful cyberattack, you should still have a plan in place that can help your team conclusively determine the precise extent of the attack or to investigate the threat in granular detail. Therefore, you need to extend your capabilities further into the incident response and remediation lifecycle.

An effective **Digital Forensics and Incident Response** service will provide much deeper cyber investigative capabilities so your team can respond to any security incident with speed and efficacy. To that end, look for an IR provider that helps your team:

- ✔ Get back to normal business operations in a matter of hours, instead of days or weeks, no matter where you are in the world
- ✔ Gain priority access to a team of elite incident responders who are highly accredited on-demand, 24/7
- ✔ Benefit from immediate time to value through remote investigations and the collection of digital forensics artifacts regardless of your organization's size or location
- ✔ Experience a smooth recovery with full support throughout the investigative lifecycle, including filing cyber insurance claims, evidence preservation, transitioning the findings to law enforcement, and strengthening your security gaps through an implementation of lessons learned

Conclusion

A successful ransomware attack or data breach can result in lasting reputational damage, major operational disruption, and significant legal and regulatory repercussions. Security leaders don't have the luxury to believe their organizations will be immune from a cyberattack, no matter the size or industry.

Studying Initial Access trends allows you to optimize multiple layers of defense for both risk reduction and cost by reviewing previous attacks and weighing potential future attack vectors.

A two-year view of incidents investigated by eSentire's Threat Response Unit reveals that the three most successful Initial Access vectors today are email, drive-by social engineering, and remote exploits. Proactively combating these risks requires:

- Implementing specific controls that prevent common malcode execution techniques
- Phishing and Security Awareness Training (PSAT) to drive behavioral change with employees and to build user cyber resiliency by understanding threat attackers' most common TTPs
- A comprehensive vulnerability management program to minimize the risk of remote exploitation
- Managed Detection and Response (MDR) to identify when a threat actor has broken through traditional defenses and to intervene before they can achieve their objectives
- Digital Forensics and Incident Response (DFIR) expertise available on retainer to provide post-incident support and emergency preparedness services

How eSentire Can Help Combat Ransomware

Every malware case mentioned in this report arrived via social engineering methods, meaning the threat bypassed primary filtering mechanisms the organization had in place in their email systems or web browsers to successfully convince a user to execute malicious code. At eSentire, we assume that your preventative controls will be bypassed so we target known TTPs associated with each stage of ransomware attacks; from initial malware deployment to intrusion actions to ransomware. Successful identification at any stage results in immediate investigation and response actions by our 24/7 SOC Analysts and Elite Threat Hunters.

eSentire is recognized globally as the Authority in Managed Detection and Response because we hunt, investigate and stop known and unknown cyber threats before they become business disrupting events. With two 24/7 Security Operations Centers, hundreds of cyber experts, and 1300+ customers, across 80+ countries, we have demonstrated the ability to Own the R in MDR with a Mean Time to Contain of 15 minutes. We deliver cyber program results through a combination of cutting-edge machine learning XDR technology, 24/7 threat hunting expertise and security operations leadership.

Why enterprises choose eSentire to defend them from ransomware threats:

- **24/7 Threat Detection and Security Operations** to disrupt ransomware attacks before they deploy across your organization
- **Battle-tested Threat Hunters and Security Experts** who manually hunt, contain and respond to ransomware attacks on your behalf
- **Our Altas XDR Platform provides Security Network Effects** so your defenses are hardened with every ransomware detection across our global customer base
- **Industry-leading threat research and detection model development** from our Threat Response Unit (TRU) to create encryption keys and new detection methodologies for lateral movement and cyber gang activities
- **Industry-leading response times.** eSentire MDR delivers a 15 minute Mean Time to Contain and our IR retainer has a 4-hour remote threat suppression SLA.

Ready to get started?

It's time to reclaim the advantage and put your business ahead of disruption.
Build a more responsive security operation today with eSentire.

Get Started

If you're experiencing a security incident or breach, contact us **+1-877-317-2414**

eSENTIRE ITSpecialist

IT Specialist Advisory Services is an IT procurement firm specializing in cloud computing, cybersecurity, and managed services. We help organizations save time, money and resources in the acquisition of information technology.

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1300+ organizations in 80+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security

operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit www.esentire.com and follow @eSentire.

References

[1] For more background on Conti, listen to Managing Cyber Risk Podcast: Leaks & Lessons - Conti's Communications Exposed [eSentire]

[2] https://attack.mitre.org/tactics/TA0001/

[3] Extracted from the TRU Positive report, IcedID to Cobalt Strike In Under 20 Minutes [eSentire]

[4] https://attack.mitre.org/software/S0154/

[5] The ransomware ecosystem is explored at length in Dissecting Today's Ransomware Ecosystem Ransomware-As-A-Service, Targeted Intrusions and Opportunistic Attacks [eSentire]

[6] For this analysis, "Other" includes abusing trusted relationships, using removable media, engaging in drive-by exploitation (as distinct from drive-by social engineering), leveraging remote access services, compromising the supply chain, and insider threats.

[7] Emotet has experienced several disruptions, but made a comeback in November 2021; in early 2022, eSentire security teams identified and disrupted multiple Emotet infections

[8] After emerging in September 2021, SquirrelWaffle gained steam throughout the year; eSentire observed multiple infections that were most likely intended to be used as staging for deployment of Qakbot and Cobalt Strike

[9] In March 2022, eSentire interrupted a suspected AsyncRAT incident that used HTML smuggling to deliver ISO files housing malicious VBS and PowerShell commands

[10] eSentire disrupted multiple SolarMarker infections throughout the latter months of 2021; in early 2022, we discovered a months-old infection in a newly onboarded customer

[11] In early 2022, eSentire observed GootLoader masquerading as a model IP security agreement, likely to target professionals in legal roles

[12] Learn more at Attack surface reduction rules overview [Microsoft]

[13] Learn more about the importance of EDR [eSentire]