The State of Zero-Day Attacks in 2021
Introduction

A zero-day vulnerability is a weakness in software known to adversaries, yet undisclosed to the vendor responsible for resolving it. As a result, there are no existing patches that users can apply to repair the vulnerability. An exploit is a piece of software, data, or a sequence of commands used to take advantage of a vulnerability. This combination of information and ability is used by cybercriminals and other threat actors to launch attacks with devastating impact to victims. Zero-day vulnerabilities are challenging for organizations of all sizes to defend against.

To a skilled adversary, zero-day exploits serve as a master key that can be used to launch crippling cyberattacks against their targets. As a result, zero-day attacks can last for weeks or months before they are detected and investigated, which can finally alert the software vendor to develop a patch.

Unfortunately, zero-days aren’t uncommon. In fact, research from Google’s Project Zero shows zero-day vulnerabilities have increased significantly in 2021 – as of November 2021, a total of 57 zero-day exploits in the wild have been discovered, compared to 25 found in 2020. Moreover, the list of zero-day vulnerabilities found in 2021 is dominated by Google, Microsoft, Apple and Adobe products relied upon by all manner of organizations. This includes the ProxyLogon vulnerabilities within Microsoft Exchange, which led to tens of thousands of organizations being at significant risk of compromise.

eSentire’s Threat Response Unit (TRU) performed a thorough analysis of zero-day vulnerabilities and how they have grown in 2021. In 2021, we detected and responded to a significant increase in zero-day exploit activity in client environments. This included defending against Solarigate, ProxyLogon, ProxyShell, and most recently, preventing further compromise of client environments that had been targeted through Kaseya’s VSA product.

TRU attributes these increases to four contributing factors:

- A growing technology footprint; as more software is written and depended on, more vulnerabilities are created as an unintended consequence of that software
- Threat actors are focusing their investments in zero-day security research - discovering vulnerabilities, developing exploits, and participating in a zero-day marketplace to purchase vulnerabilities and weaponized exploits
- Mature threat hunting and detection programs have improved efficacy towards identifying zero-day attacks
- Security researchers are publicly disclosing more zero-day vulnerabilities before vendors have made software updates available

A zero-day attack cannot always be prevented (e.g., by patching). In combination with other security and risk mitigation controls, your organization’s ability to withstand a zero-day attack is dependent upon its capacity to detect and respond to an incident post-exploitation. This fact is true for a genuine zero-day exploit and for the period between an exploit becoming known and a patch becoming available.

Managed Detection and Response (MDR) is a major differentiator when it comes to protecting organizations against zero-day attacks. Of course, detection and response capabilities both require visibility across as much of the IT environment as is possible, including endpoints, log, network, and cloud environments. eSentire MDR has enhanced visibility and monitoring in place to identify threat actor behaviours, including post-compromise activity.

In multiple cases in 2021, eSentire’s TRU was able to mitigate zero-day impacts prior to a vendor releasing an update to address the zero-day vulnerability due to having detections in place for post compromise activity. Threat actors will use zero-day exploits as new attack vectors but are consistent with their Tactics, Techniques, and Procedures (TTPs) once initial access has occurred and an environment is compromised.
Defining Opportunity Windows for Zero-Day Exploits

Zero-day exploits are rarely prevented, but follow-on intrusions can be detected and responded to in a way that minimizes the impact of these incidents.

To assess the challenge of zero-day vulnerabilities in 2021, TRU reviewed zero-day vulnerabilities and defined opportunity windows for threat actors to leverage their zero-day exploits.

The first opportunity window, called **patch delay**, relates to the threat actor’s opportunity to exploit an unpatched zero-day vulnerability (Figures 1 and 2). This opportunity usually belongs to a small group of threat actors who have the knowledge and capabilities to create and leverage an exploit while the rest of the world is unaware of the vulnerability.

*Figure 1: Time delay between exploitation and availability of working patches for high-impact vulnerabilities*

*Figure 2: Patching Delay over 2021*
Research from TRU shows in 2021, it has taken vendors less than three weeks to release a patch following the first exploitation attempt of the zero-day vulnerability by threat actors. Over the course of the year, vendors began to develop and release patches faster, which means threat actors have had less time to weaponize the vulnerabilities. However, this has also meant these threat actors have evolved to move faster to beat the time-to-patch window.

The second opportunity is time-to-patch, which is a vulnerable organization’s opportunity to defend against a zero-day vulnerability. This measure reflects the time delay between the announcement of a zero-day vulnerability and the widespread exploitation of the vulnerability.

When it comes to zero-day vulnerabilities, and particularly when patches are simultaneously unavailable, yet the product is widely used, the impact against businesses can be pervasive and severe. Zero-day exploits often lead to cryptocurrency coin mining or ransomware payloads being deployed in compromised environments as well as data exfiltration from the victim environment.

Research from TRU has shown in 2021, organizations had approximately one week to patch zero-day vulnerabilities before they were actively exploited in the wild (Figures 3 and 4).
Detecting and Responding to Zero-Day Exploits

Since the value of a zero-day exploit is immense for any highly skilled adversary, they will prioritize widely used technology (e.g., Exchange servers) for exploit development. This can sometimes result in a single Advanced Persistent Threat (APT) leveraging a zero-day exploit against many victims while the zero-day vulnerability is unknown to the public. Therefore, it’s critical an organization can detect and respond to any activities following initial exploitation.

Research from TRU has also shown that although threat actors will use zero-day exploits as new attack vectors, they will remain consistent with their TTPs once an environment is compromised. So, while your organization may not be able to prevent all zero-day exploits, it’s likely the follow-on intrusions can be detected and prevented.

There is also a critical need for continually updated detections to allow security teams to respond directly to zero-day attacks. Having these detections in place for post-compromise TTPs will minimize the risk of zero-day exploits not being detected and causing a business disrupting event.

For example, eSentire’s TRU team has been able to prevent further exploitation of ProxyShell and most recently, our team detected, responded, and prevented further compromise of client environments during the Kaseya VSA incident due to having detections in place for post compromise activity.

The following case studies demonstrate the value of having eSentire MDR with improved detection, 24/7 threat hunting, deeper investigation, and complete response for zero-day attacks.

While your organization may not be able to prevent all zero-day exploits, it’s likely the follow-on intrusions can be detected and prevented.
Case Study:
ProxyLogon & ProxyShell Zero-Days

The timeline of the ProxyLogon zero-day vulnerability illustrates where vulnerability management programs fall short, and how eSentire’s TRU team detected and responded to minimize the impact of zero-day exploits.

The ProxyLogon zero-day vulnerabilities were discovered on December 31st, 2020 and in March, Microsoft reported the APT, HAFNIUM, was behind the closed exploitation that had occurred prior to public disclosure.

On March 1st 2021, eSentire began detecting post compromise WebShell activity. Once Microsoft disclosed the vulnerability, eSentire’s TRU began a Global Threat Hunting operation. As a result of the Global Threat Hunt, 22 true positives were detected and remediated in customer environments.

Table: Timelines of ProxyLogon & ProxyShell

<table>
<thead>
<tr>
<th>Targeted Use</th>
<th>Web Shell Spray</th>
<th>Widespread Opportunistic Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 31st</td>
<td>January 5th</td>
<td>March 11th</td>
</tr>
<tr>
<td>DEVCORE</td>
<td>December 31st</td>
<td>Microsoft Discloses Vulnerability</td>
</tr>
<tr>
<td>Creates Working Exploit</td>
<td>Reported to Microsoft</td>
<td>DearCry aka DoejoCrypt Ransomware</td>
</tr>
<tr>
<td>January 3rd</td>
<td>March 1st</td>
<td>March 10th</td>
</tr>
<tr>
<td>Earliest Webshell Observation (Volexity)</td>
<td>Earliest Webshell Observed by eSentire</td>
<td>PoC Release</td>
</tr>
<tr>
<td>March 15th</td>
<td>March 18th</td>
<td>March 18th</td>
</tr>
<tr>
<td>LemonDuck</td>
<td>BlackKingdom aka Pydomer Ransomware</td>
<td>aka Pydomer Ransomware</td>
</tr>
</tbody>
</table>

Successfully completing this threat hunting operation required:

1. Actively monitoring the threat landscape and having awareness of client’s assets
2. Identifying post compromise activity
3. Working with the vendor to leverage custom tools they developed for detecting the zero-day vulnerability
4. Providing mitigations and remediation support when patching wasn’t immediately available

A similar outcome resulted from ProxyShell exploitation later in the year. Again within days of disclosure of the ProxyShell zero-day vulnerability, eSentire began to detect and mitigate attacks exploiting this flaw.
Case Study: 2021 Kaseya VSA Zero-Day

Prior to the 4th of July holiday weekend in 2021, eSentire’s TRU team became aware Kaseya may have been the victim of a supply chain attack. Initial response included the TRU team collecting and validating Indicators of Compromise (IoCs) which were then added to the Threat Intelligence Platform for processing and development.

Once reports of mass exploitation of Kaseya’s VSA product were confirmed, TRU moved within 30 minutes to weaponize early IoCs collected and initiated Global Threat Hunts across the entire client base. As a result of these Global Threat Hunts, a positive threat detection was discovered and revealed at least one customer had been impacted by the Kaseya VSA zero-day.

With the support of eSentire’s TRU team, eSentire’s Security Operations Center (SOC) Cyber Analysts isolated impacted endpoints to prevent any lateral movement, remediate, and return impacted systems to service.

While global threat hunts were occurring, eSentire’s TRU team also informed customers of this hunt through a global security advisory, which contained information on what eSentire was doing about the discovery of the Kaseya VSA zero-day that was disseminated to all customers.

By that evening, eSentire SOC Cyber Analysts had isolated and remediated known malicious hashes across our MDR for Endpoint customers, which effectively protected all endpoints across our customer base from any Kaseya VSA zero-day exploit.

eSentire’s team of SOC Cyber Analysts performed 24/7 monitoring and investigation for impacted customers throughout the July 4th weekend, while TRU continually worked to immediately identify any new IoCs.

Within 24 hours, a machine-learning powered Atlas XDR detection was pushed across all MDR for Endpoint customers, automating threat detections for Kaseya VSA zero-day exploitation to protect clients from potential Kaseya VSA based compromises. On the same day, a new investigation runbook was deployed for our SOC Cyber Analysts to use for any new detections and human-led investigations.
Conclusions

In 2021, eSentire detected and responded to a significant increase in zero-day exploit activity in client environments. This included defending against Solarigate, ProxyLogon, ProxyShell and most recently preventing the further compromise of client environments that had been targeted through Kaseya’s VSA product. From our analysis, it’s clear threat actors will continue to leverage zero-day exploits to launch cyberattacks and create operational disruption within an organization.

While a genuine zero-day exploit can rarely be detected, it’s important to note threat actors still follow the same tactics, techniques, and procedures (TTPs) to deploy any malicious payload. Therefore, your organization still needs complete visibility into your assets in addition to 24/7 threat detection and response capabilities so it’s possible to detect known tradecraft post-exploit.

Unfortunately, very few organizations have the in-house expertise and resources needed to defend against today’s highly advanced and potentially devastating zero-day threats. As such, we strongly recommend organizations:

- **Adopt a comprehensive vulnerability management program:** All too often, organizations fail to do so despite having a patch available. So, it’s critical to proactively do vulnerability scanning as part of a comprehensive vulnerability management program to enable your team to understand which systems are inadvertently exposed and have a disciplined approach to patch management. As soon as a vendor releases a patch, your security team must review and apply it immediately.

- **Operationalize information to bolster response:** Your team must be able to aggregate all available information on specific vulnerability and apply actionable intelligence to mitigate risk. As such, ensuring a strong defense against zero-day threats requires security teams to respond fast and continually bolster detection and response capabilities.

- **Actively review Indicators of Compromise (IoCs):** In parallel to automatically blocking malicious activity, your team must stay on top of tracking any IoCs to reveal if an attacker has bypassed any security defenses. However, this typically requires technical expertise (e.g., security practitioners must know how to use logs, endpoint telemetry, and anomaly detection) that may extend beyond the skillset of an IT team lacking security specialists.

- **Engage a Managed Detection and Response (MDR) provider:** One key differentiator in protecting your organization against zero-day exploits is multi-signal MDR that provides enhanced visibility into the full attack surface with 24/7 threat detection and response. This will position your team to mitigate the impact of a zero-day threat by enabling you to identify when a threat actor has broken through traditional defenses and intervene before they can achieve their objectives.
How eSentire MDR Can Help Protect Against Zero-Day Threats

eSentire MDR has enhanced visibility and monitoring in place to identify threat actor behaviours, including post-compromise activity. With multi-signal attack surface coverage, powered by a strong XDR platform foundation and human expertise to identify, contain, and respond to threats bypassing existing defenses 24/7.

eSentire is recognized globally as the Authority in Managed Detection and Response (MDR) because we hunt, investigate, and stop cyber threats before they become business-disrupting events. We go beyond the market’s capability in threat response. eSentire’s multi-signal MDR approach ingests endpoint, network, log, cloud, asset, and vulnerability data that enables complete attack surface visibility.

Enriched detections from the eSentire Threat Response Unit are applied to captured data identifying known & unknown threats, including suspicious activity and zero-day attacks. With two 24/7 Security Operations Centers staffed with cyber experts and Elite Threat Hunters, an industry-leading XDR Cloud Platform, and refined security operations processes, eSentire can detect and respond to cyber threats with a Mean Time to Contain of 15 minutes.

Ready to get started?

Connect with an eSentire Security Specialist to learn more about how eSentire Multi-Signal MDR, powered by our Atlas XDR Cloud Platform, can deliver security that scales across your organization.

Contact Us

If you’re experiencing a security incident or breach contact us 1-866-579-2200

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries 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.