COLORTOKENS

THREAT RESEARCH

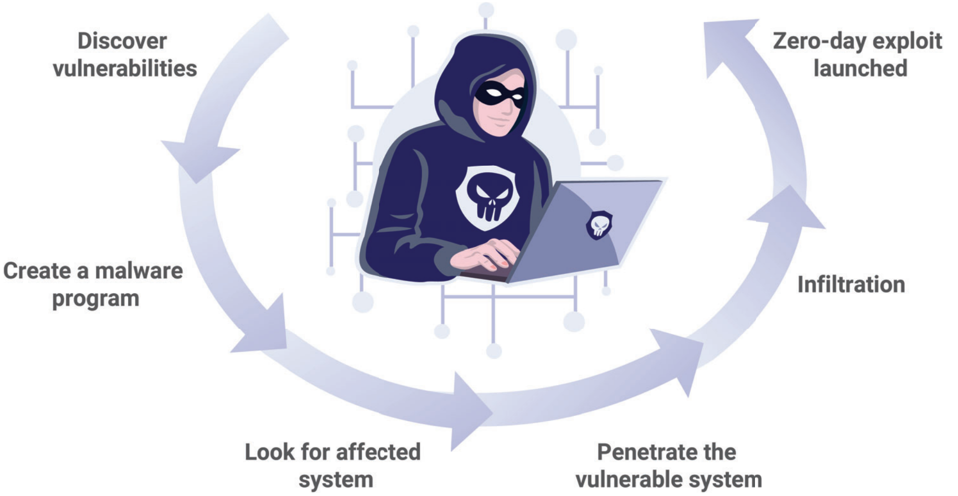
Defensive Strategy Against The Perils Of Zero Day Exploit

Over the last few years, Organisations are finding it tough to keep up with the volume of potential threats and severity of advanced attack vectors, especially with traditional security measures in place. In this scenario, while the success rate of containing a known threat is still high, the real struggle begins when security professionals have to handle emerging threats that take advantage of unknown vulnerabilities in software. Such attacks are referred to as “Zero Day Exploit” that leverages a zero-day vulnerability for which patches are not available and occurs on the zero day of awareness when no defences are in place.

Zero-Day Exploit becomes really dangerous when cybercriminals reserve undiscovered vulnerabilities for future use against high value targets, thereby increasing the lifespan of the exploit. But, once a zero-day vulnerability is brought to a software company’s attention, a security patch could be created and released, post which the exploit is no-longer called “Zero-Day”. Normally, these actions follow as soon as a software vulnerability is found[1]–

1. A vulnerability in code is released as part of a software application.
2. Attackers find a way to attack vulnerable systems through the newly discovered vulnerability
3. Vulnerability is discovered by vendor, but a patch is still not available.
4. Vulnerability is disclosed publicly, making both users and attackers widely aware of it.
5. Anti-virus vendors identify the attack signature and protect against it.
6. A patch is released by the vendor that fixes the vulnerability.
7. Application of the patch is completed by software users.

But, before these patches are developed, distributed and applied on applications, systems are still vulnerable throughout the entire period , giving the attackers an additional advantage of time to deploy their malware through the vulnerabilities and compromise scores of devices or network. Attackers normally follow a 6-step approach to target their victims:



An empirical study has shown that the average window of exposure for a zero day attack is ten months. Throughout this window of exposure, a race begins among attackers, vendors and users with attackers trying their best to make it to the affected system before a patch is deployed and antivirus system is updated by organizations.

Latest Zero Day Exploits Observed

Identifying zero-day vulnerabilities and preventing zero-day attacks is of utmost priority to all the security researchers and professionals. Some notable zero-day attacks, such as Stuxnet, Duqu, Flame, Downadup, Fujacks, Ramnit, have shown us how easy it is for attackers to bypass traditional security signature-based measures. To improve the security posture of an organization, it's imperative to reflect on the following latest trends in Zero-Day Exploit[2]:

SEP 2020

Zero Day Flaw in the File Manager, a popular Word Press Plugin, found to be actively exploited, affecting some 700,000 WordPress sites.

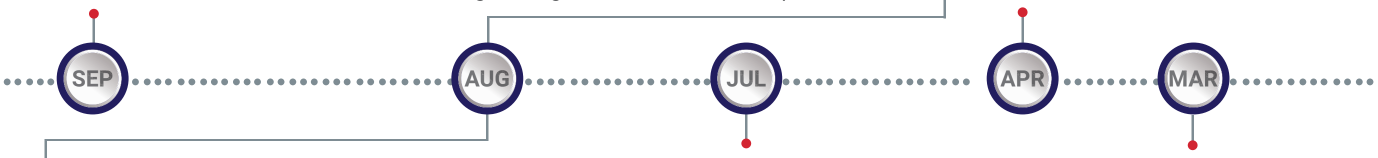
AUG 2020

Security Shortcomings in Apple's Safari browser created zero-day vulnerability that could be harnessed in social engineering attacks.

Security researchers identified a sophisticated strain of XCSSET, Apple Mac Malware, that targets Xcode software developers.

APR 2020

Zero-day attacks were reported against the Sophos' XG firewall to exploit a SQL injection vulnerability (CVE-2020-12271) targeting the firewall's built-in PostgreSQL database server.



A zero-day vulnerability in vBulletin forum software was disclosed that can be exploited to launch remote code execution (RCE) attacks.

Security researchers found that the flaws in the Windows print spooler component were still exploitable using fresh techniques, a decade after Stuxnet.

JUL 2020

Unpatched Tenda WiFi router vulnerabilities leave home networks wide open to abuse.

MAR 2020

Microsoft warned users of zero-day attacks exploiting two separate vulnerabilities - Remote Code Execution (RCE) vulnerabilities in the Adobe Type Manager (ATM) library & IE scripting engine.

Effective Response Requires A Next-Gen Approach

Real time detection and mitigation of zero-day attacks is no more possible with signature-based antivirus. Organizations that want to defend & actively respond against the most stealthy and advanced cyberattacks will have to keep a next-generation, multi-layered defence system in place.

The research community from SANS Institute has broadly classified the defence techniques against zero-day exploits as statistical-based, signature-based, behaviour-based, and hybrid techniques with a single motto to identify the exploit in real time and quarantine the specific attack to eliminate or minimize the damage caused by the attack[3].

1 Behaviour-based Detection

depends on the analysis of the exploit's interaction with the target. While often based on analysis of data captured using high interaction honeypots, normal interactions can be learned, future activity predicted, and exploits can be classified into behavioural groups. Interactions outside the normal behaviour groups would be suspicious and quarantined. This method, thus, has the potential to detect and analyse potential zero-day exploits in real time

2 Statistical-based Detection

relies on attack profiles built off of historical data. This approach does not usually adapt well to changes in zero-day exploit data patterns. Any changes in a zero-day exploit's pattern would require a new profile to be learned by the system.

3 Signature-based Detection

dependent on signatures made from publicly known exploits. These signatures will defend against some variations of the original signature or exploit depending on the process used by the attackers to conceal the original known exploit's signature.

4 Hybrid Detection Model

combines models previously mentioned using a heuristic approach and will depend on what other methods of detection are combined in the environment

From the above definitions, it's clear that not one but a unified approach involving all the above techniques would guarantee a proper detection & mitigation of each stage of a Zero-Day Exploit. Without these capabilities, a zero-day attack on your system can stay well under the radar before its damaging effects reveal themselves.

ColorTokens can effectively tackle Zero-Day Exploit

Understanding that real time vigilance and persistence is necessary to detect vulnerabilities and contain zero-day attacks, ColorTokens has created a holistic view towards security against zero-day attacks by combining the above mentioned detection models and introducing the following solutions and services that enhance your security posture in real time -

Xshield

Based on Statistical and Signature based detection models, provides round the clock visibility and helps in creating rules

Xprotect

Based on Behavior and Hybrid based detection models, helps in creating rule rings and customize them

With the help of above products and services, ColorTokens can effectively defend against each attack stage in the following manner:

Zero Day Activities	ColorTokens Coverage
Attackers Identify vulnerabilities in the systems	**Xshield** capable of identifying open ports and existing vulnerabilities.
Plan and deploy Malware to exploit Zero-Day vulnerabilities	**Xprotect** identify and prevent new malicious process execution with Threat Intel capabilities
Unknown new process / unusual execution behavior	**Xshield** offers Micro-segmentation which can identify and block unusual and malicious connections
Unusual connections and lateral movements to various systems by exploiting vulnerable services	**Xprotect** identify and prevents unknown/suspicious processes using rule rings

To learn more about how our solutions can defend against Zero Day Malware , please watch this video

▶ Watch Now

References

[1] https://www.getadvanced.net/technology-blog/article/understanding-zero-day-threats-and-their-importance-in-security-strategy
[2] https://portswigger.net/daily-swig/zero-day
[3] https://www.sans.org/reading-room/whitepapers/bestprac/defenses-zero-day-exploits-various-sized-organizations-35562

ColorTokens Inc., a leader in proactive security, provides a modern and new generation of security that empowers global enterprises to singlehandedly secure cloud workloads, dynamic applications, endpoints, and users. Through its award-winning cloud-delivered solution, ColorTokens enables security and compliance professionals to leverage real-time visibility, workload protection, endpoint protection, application security, and Zero Trust network access—all while seamlessly integrating with existing security tools. For more information, please visit www.colortokens.com