APPGUARD
The Malware Disruptor

Prevent Zero-Day Attacks with The Right Defense:

Preparing for the Next MS Exchange Attack

WHITE PAPER

SUMMARY:
Zero-day attacks are difficult but not impossible to defend against. This paper outlines the zero-day attack threat and why traditional endpoint protection tools are ineffective at protecting against these attacks. Find out how the Microsoft Exchange Server attack unfolded and the steps you can take to prevent becoming a victim to zero-day attacks.

The Zero-Day Attack Threat

Zero-Day attacks are not new. For some time now, hackers have realized that software programs are vulnerable and that unintentional flaws in software can be exploited to bury malware that can be used to access otherwise secure data. Malicious code can sit unnoticed within an environment for days, months, or years collecting sensitive data without being detected. Zero-day vulnerabilities are one of the most common and most difficult attacks to protect against.

Software programmers are always on the lookout for vulnerabilities in their software, and when a flaw is discovered they issue patches to fix the vulnerability. By sending out that patch, however, the programmer is announcing to the world where flaws exist. Often, hackers see this as an opportunity to cause harm before users have time to implement the patch. Hackers also proactively seek to find vulnerabilities in programs - often finding them before software programmers. In essence, software developers and users have zero-days to fix a flaw before it becomes a potential exploit opportunity for hackers.

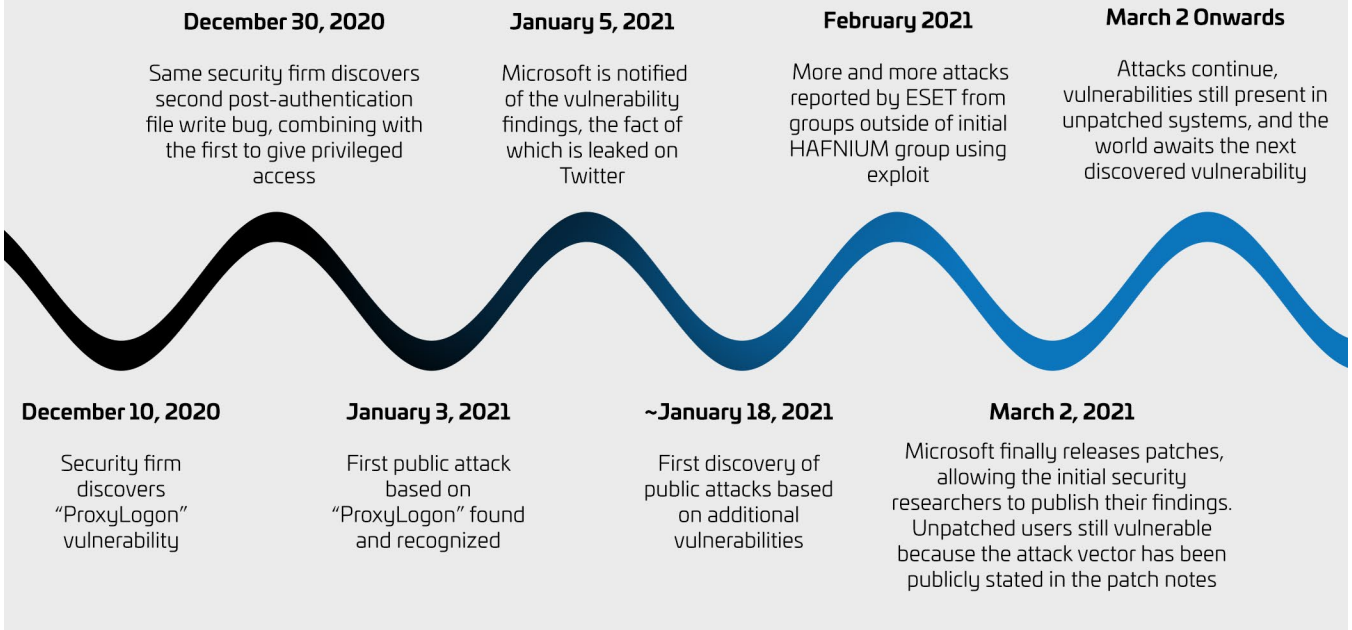
The recent Microsoft Exchange Server attack is yet another reminder of just how vulnerable software is. Like many zero-day attacks, the Microsoft Exchange Server attack, attributed to a Chinese operator called HAFNIUM, was a multi-vector attack. While the attack was detected and reported in early January of 2021, Microsoft was unable to release a patch until March 2nd – giving attackers months to exploit weaknesses to indiscriminately infect servers. By the time of the patch, many systems were already compromised. In fact, it is estimated that tens of thousands of entities across the globe were infected.

Understanding the Microsoft Exchange Server Attack

The Microsoft Exchange Server attack was a multi-prong attack that used multiple attack vectors. First, they gained access to an Exchange Server by using stolen passwords or previously undiscovered vulnerabilities to impersonate someone with access privileges. The attacker then created a web shell to take control of the compromised server. Having access to the server, the hacker was able to steal data from the organization's network. In essence, the attacker targeted the unified messaging function of Microsoft Exchange's code to remotely launch code to install web shells to gain persistent access to the system. The installation of web shells granted hackers administrator rights, opening up multiple avenues of compromise, including credential harvesting and lateral movement to other systems. Such multi-prong attacks are often referred to as malware cocktails.

Attack Timeline

"Discovery" Is Not Protection



> *AppGuard enforces the normal behaviors of the host system, employing a combination of control mechanisms which create roadblocks and disrupt the path of malware at various different stages of its potential attack, defending without having to recognize malware or its effects.*

Why Traditional Tools Cannot Defend Against Zero-Day Exploits

If nothing else, the impact of the Microsoft Exchange Server attack proved that traditional security measures fail against zero-day attacks. The attack's use of remote code execution that did not require authentication of any kind allowed attackers to penetrate software without being detected by traditional security measures – including anti-virus, Endpoint Protection Platforms (EPP), and Endpoint Detection and Response (EDR) solutions. Given traditional anti-virus and next generation anti-virus tools detect breaches by identifying known malicious code, or code that is not on their trusted default list, malicious code embedded in software is impossible to detect by these tools.

The same is true with Endpoint Detection and Response (EDR) and Endpoint Protection Platform (EPP) solutions, as these tools focus on detecting attacks on endpoints based on extrapolating previous threat behaviors to predict current or future threats. This method catches some threats but misses others when they are sufficiently unique in nature. Plus, even when EDR "catches" a threat it shows up on a logging system buried in a slew of false positive threat reports, requiring a heavy burden of forensic analysis to discover which alerts are actionable or not. The delayed response time can mean the difference between being compromised or not, depending upon how quickly the attacker strikes.

Defend Against Zero-Day Attacks with AppGuard

AppGuard is different. Instead of trying to stop applications from being exploited, it renders hijacked applications harmless, thereby stopping malware from achieving its desired goal. It does so by enforcing real-time security protocols that are not reliant on detecting the behavior of malware, determining good vs. bad, or generating alerts requiring humans to investigate. Instead, AppGuard enforces the normal behaviors of the host system, employing a combination of control mechanisms which create roadblocks and disrupt the path of malware at various different stages of its potential attack, defending without having to recognize malware or its effects. The result of this approach is that when malware uses new patterns, or exploits brand new vulnerabilities, AppGuard's security efficacy is equally as strong and is not playing catch up - making it uniquely suited to defend against zero-day and sophisticated polymorphic attacks.

AppGuard's Zero Trust endpoint protection makes use of patented launch restriction, containment, and isolation techniques to dynamically control the behavior of applications and utilities. Instead of trying to keep up with the constant evolution of malware, it keys in on restricting the finite high-risk actions necessary for malware to do its job, such as risky registry modifications, memory read/write access, or unauthorized information extrusions. Applying its controls adaptively based on context, AppGuard provides maximum security while still allowing for normal operations so work can get done.

This multi-layer defense usually disrupts the earliest stages of often undetectable cyber attacks, including zero-day malware, phishing, weaponized documents, "malvertising", watering holes, fileless malware, drive-by-downloads, ransomware, memory scrapers, and other escalating attacks that conventional security approaches can't and don't stop. However, the power of AppGuard is that it applies its controls over malicious activities that are necessary in both early and late stages of attacks, allowing multiple opportunities to block its success.

AppGuard's patented approach uniquely blends simple and easy to manage policy controls that dynamically block unacceptable, yet deterministic actions. While adversaries can easily change how malicious code looks and behaves, changing what actions it takes is extremely rare. Endpoint attackers cannot achieve their goals without successfully executing certain finite actions. AppGuard disrupts them.

How AppGuard Thwarted the Microsoft Exchange Server Attack: A Real Life Example

AppGuard's adaptive policy controls protected AppGuard customers and neutralized the Microsoft Exchange Server attack by applying roadblocks to the action the Exchange server attempted to make after being hijacked. Operationally, AppGuard automatically adapts to application changes, as well as unanticipated attack variations. In the case of the Exchange Server attack, a customer with AppGuard – whether installed just recently or five years ago – would have been protected against the attack with AppGuard's default policies. As noted earlier, the Microsoft Exchange Server attack was a multi-pronged "malware cocktail," and multiple aspects of AppGuard's controls combined to block its success.

Containment policy over the Exchange Server

AppGuard's containment policy blocks contained applications and utilities from making alterations or reading/writing to memory on system resources, with exceptions available for specific needs. In this case, AppGuard's default configuration:

- Blocked the attempted exploit write operations to
  - "C:\inetpub\wwwroot\"
  - %PROGRAMFILES%
- Blocked read operations of Local Security Authority Subsystem Service ("LSASS" - a core Windows security process) attempting to steal credentials
  - If this didn't happen due to a configuration exception by the administrator, it would block in a later stage of the attack when the credential dump writes to
    - C:\windows\temp\
    - C:\root\

Isolation policy over LSASS

Isolation policy blocks access to memory and control over high value system resources, with only specific exceptions allowed for operational necessity as configured by an administrator. Exchange would not need such exceptions and so this policy would apply.

- Since LSASS is a high value resource, by default it would have Isolation policy applied. Therefore, if a containment exception applied (i.e. to get around the previous policy) Isolation would step in and block access and the ability to gain security credentials.

Zero Trust Space Launch/Load Controls

This policy separates the host system into high value vs. untrusted space (i.e. areas with (a) few if any restrictions on what files may be there or be changed and (b) have high access to the outside world, such as user profile, desktop, downloads, etc.). Scripts and utilities launching from untrusted space locations are blocked. Additional launch and load controls are available to reduce the attack surface, prohibiting the use of certain high-risk utilities except in very specific circumstances, since those utilities are used commonly in living off the land attack techniques. Here, AppGuard:

- Blocked the attempt to add user accounts because the respective utility is restricted
- As Exchange Server attempted to write malicious executables, scripts, or DLLs to folders where AppGuard normally allows writes (i.e., does not have Isolation applied to the area), AppGuard still blocked them from running because they were attempting to launch from an untrusted space. For example, PowerCat was loaded via a malicious DLL and AppGuard blocked it because it was doing so from an untrusted location targeting a high value location.

Non-default Isolation Additions

Some customers use additional policies and apply AppGuard isolation rules to prevent installation of snap-ins by essentially locking select registry keys, allowing only select configuration applications to alter them or only allowing changes during maintenance windows. The additional policies would have also blocked the activities the attack used to gain its foothold and steal information.

> *"When malware uses new patterns, or exploits brand new vulnerabilities, AppGuard's security efficacy is equally as strong and is not playing catch up - making it uniquely suited to defend against zero-day and sophisticated polymorphic attacks."*

AppGuard should be your first and main line of defense in an increasingly dangerous cyber and human threat environment.

Mark Kelton
Former Deputy Director for Counterintelligence, CIA

These examples demonstrate the benefit of AppGuard's true preventative techniques, applying redundancies and roadblocks to the dangerous activities that malware will attempt to execute in the process of an attack.

By taking an agnostic approach to the "how", and instead focusing on the "what", AppGuard closes the inherent holes within any application configuration that attackers will always try to take advantage of. An additional benefit of this approach is that within the few holes that are left in the interest of operational efficiencies, the load on detection tools is significantly reduced, allowing them to be more accurate and more efficient in catching malicious acts early, thereby reducing the number of alerts and human resource costs.

Protect Against Zero-Day Exploits

Zero-day exploits are not going away. Cyber attacks that target trusted applications are highly-scalable with widespread implications. The Microsoft Exchange Server attack has impacted businesses, governments, and cybersecurity teams around the globe. Attackers continuously hone their craft, and nation-state sponsored attackers are more determined than ever to cause harm. Organizations must increase their foundational cyber security capabilities and deploy tools that can protect against a wide range of attacks, including zero-day. AppGuard, with its patented endpoint protection technology, was built to prevent the most advanced attack techniques, including those employed in recent high profile attacks.

About AppGuard

AppGuard is a cyber security company on a mission to set a new standard: true cyber protection for all. AppGuard's patented technology prevents compromises before they happen by disrupting malware activity from causing harm without having to recognize it. Unlike detection-based solutions, AppGuard outsmarts malicious actors to ensure businesses can do what they need to do, and malware can't do what it wants to.

APPGUARD
The Malware Disruptor

www.appguard.us | sales@appguard.us