Lodestone

SEPTEMBER 2022

STATE OF CYBER

monthly newsletter

THE FUTURE OF SECURITY NOW: BEHAVIORAL DETECTION

There is nothing static about the world of cybersecurity. Threat actors have progressed by leaps and bounds since hackers and breaches first began to make popular headlines. The minimum security standards, too, have evolved to give companies a fighting chance against increasingly advanced tactics.

Traditional anti-virus (AV) relies on a defined set of signatures to detect malicious activity. It compares these signatures to files on a system to determine if a file is bad. While this set of signatures is continually updated, the result is often a game of catch-up for security professionals and AV customers alike. The latest technology instead poses this question: what if the file isn't inherently malicious, but is involved in a malicious activity? Furthermore, what if harmful behavior isn't tied to a file at all?

Behavior-based detection is the modern standard for security as traditional AV becomes obsolete. **In fact, the vast majority of malware and malicious activity Lodestone's Digital Forensics and Incident Response (DFIR) team has investigated was not detected by the traditional AV solutions the victims had in place.** The main solution to this problem is two-fold: next-generation AV (NGAV) and endpoint detection and response (EDR).

NGAV combines the best of traditional, signature-based monitoring with real-time process monitoring to provide a clear view of an organization's security landscape. EDR takes this one step further by providing a centralized management console from which administrators can act by connecting to their networks to monitor, investigate, and respond to incidents and take advantage of a plethora of features.

Still unsure if behavior-based detection is necessary for your organization? Remember this: in almost every network breach Lodestone has investigated, correctly implemented NGAV and EDR solutions would have prevented the attack or dramatically reduced the damage it caused.

BLACKBYTE RANSOMWARE GANG RETURNS WITH TWITTER PRESENCE, TIERED PRICING

Ransomware groups continue to increase the pressure on their victims by reducing the time they have to pay ransoms before their data goes public. Ensure that your organization's communication plan outlines a clear and decisive response to such events.

35,000 REPOS NOT HACKED, BUT CLONES FLOOD GITHUB TO SERVE MALWARE

Cloned GitHub repositories ("repos") have been utilized to trick high volumes of users into unwittingly downloading malware. Protect your users and your organization by ensuring that only trusted GitHub repositories are used.

NORTH KOREA HACKERS SPOTTED TARGETING JOB SEEKERS WITH MACOS MALWARE

The North-Korea-backed Lazarus Group has been observed targeting job seekers with malware capable of executing on Apple computers with Intel and M1 chipsets. It is critical to be aware that Mac computers are not immune to security events: organizations must ensure that they have the same level of protection as Windows endpoints.

STATE-SPONSORED APTS DANGLE JOB OPPS TO LURE IN SPY VICTIMS

Phishing attackers targeting individuals searching for jobs are on the rise. Be aware of this trend and continue to educate your workforce on the latest phishing campaigns and tactics.