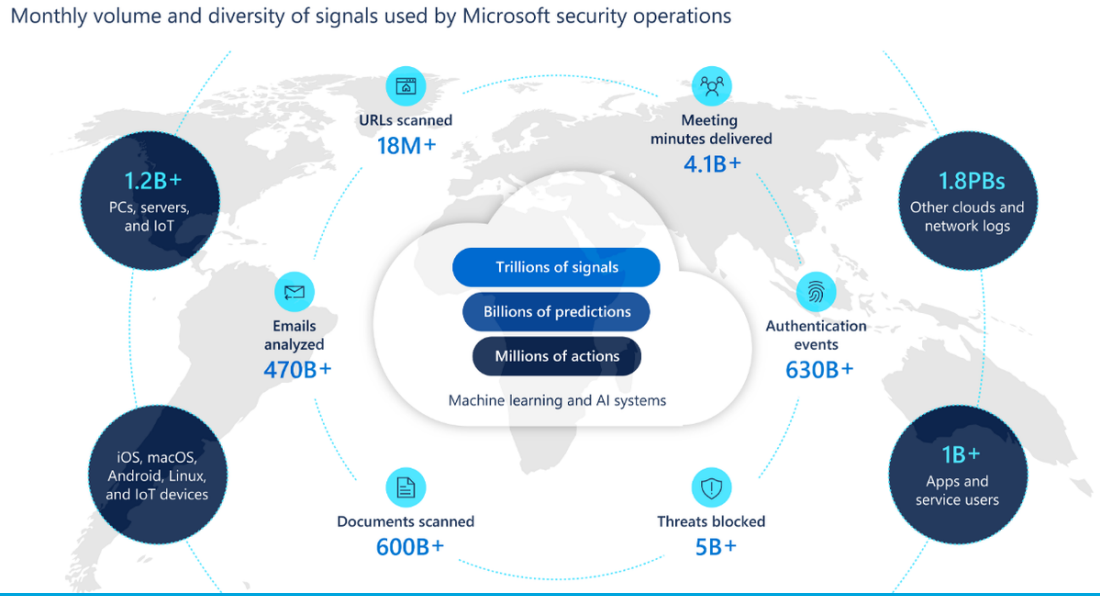
kindred

Security Newsletter

5 October 2020

Subscribe to this newsletter

Microsoft Digital Defense Report 2020: Cyber Threat Sophistication on the Rise



Microsoft is releasing a new annual report, called the Digital Defense Report, covering cybersecurity trends from the past year. This report makes it clear that threat actors have rapidly increased in sophistication over the past year, using techniques that make them harder to spot and that threaten even the savviest targets.

n addition to attacks becoming more sophisticated, threat actors are showing clear preferences for certain techniques, with notable shifts towards credential harvesting and ransomware, as well as an increasing focus on Internet of Things (IoT) devices. Among the most significant statistics on these trends: In 2019 we blocked over 13 billion malicious and suspicious mails, out of which more than 1 billion were URLs set up for the explicit purpose of launching a phishing credential attack. Ransomware is the most common reason behind our incident response engagements from October 2019 through July 2020. The most common attack techniques used by nation-state actors in the past year are reconnaissance, credential harvesting, malware, and Virtual Private Network (VPN) exploits. IoT threats are constantly expanding and evolving. The first half of 2020 saw an approximate 35% increase in total attack volume compared to the second half of 2019.

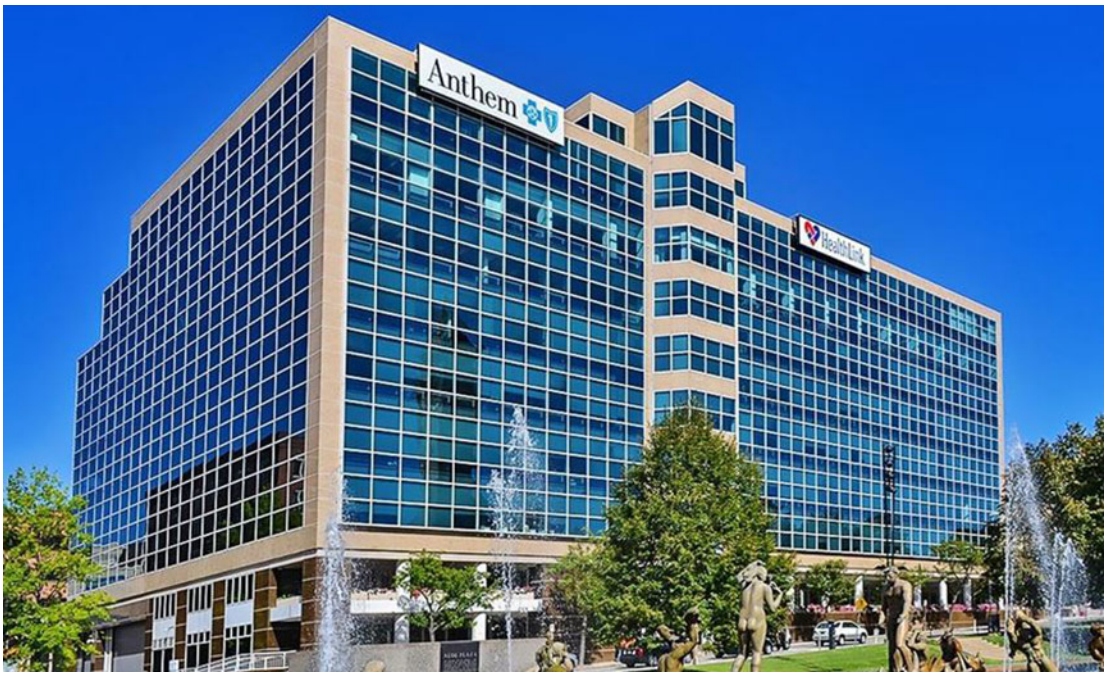
All in all, Microsoft concludes that criminal groups have evolved their techniques over the past year to increase the success rates of their campaigns, as defenses have gotten better at blocking their past attacks. Just like in years prior, the entire cybersecurity landscape appears to be sitting on a giant merry-go-round, and constant learning and monitoring is required from defenders to keep up with the ever-evolving attackers, may them be financially-motivated or nation-sponsored groups.

Read More on ZDNet

Microsoft Digital Defense Report 2020

Anthem Hit With $48 Million in Additional

Breach Penalties



The attorneys general of 41 states, plus Washington, D.C., have slapped health insurer Anthem Inc. with a $39.5 million settlement in the wake of a 2014 cyberattack that affected nearly 79 million individuals. Meanwhile, the attorney general of California signed a separate but similar $8.7 million settlement with the health insurer. The settlements announced Wednesday follow a $115 million settlement Anthem signed in 2018 to resolve a consolidated class action lawsuit, plus a record $16 million HIPAA settlement that same year with the Department of Health and Human Services' Office for Civil Rights.

In 2015, Anthem revealed a data breach exposing the personal information of 78 million consumers, including over 13.5 million Californians, the California statement notes. The data included names, addresses, email addresses, Social Security numbers, healthcare identification numbers and dates of birth. Hackers sent targeted phishing emails containing malware to Anthem's employees to steal credentials so they could access the insurance company's network, and then they spent months stealing information from Anthem's most sensitive database containing consumers' personal information, the California statement notes.

According to the California attorney general, an investigation into the incident found Anthem had numerous security deficiencies, including the failure to limit access to computers holding sensitive information, protect account credentials and passwords from unauthorized use, update security tools and adequately log and monitor network activity to detect malicious activity. "When consumers must disclose confidential personal information to health insurers, these companies owe their customers the duty to protect their private data," Becerra said. "Anthem failed in that duty to its customers. Anthem's lax security and oversight hit millions of Americans. Now Anthem gets hit with a penalty, in the millions, in return." Under the settlement with California, as well as the multistate settlement, Anthem has agreed to take a number of corrective actions to improve its data security practices. In its statement, the New York attorney general's office says Anthem's corrective actions include Implementing a comprehensive information security program that incorporates principles of "zero trust" architecture and includes regular security reporting to the board of directors and prompt notice of significant security events to the CEO.

Read More on BankInfoSecurity

More #News

- Microsoft Windows XP Source Code Reportedly Leaked Online
- Pastebin adds 'Burn After Read' and 'Password Protected Pastes' to the dismay of the infosec community
- KuCoin cryptocurrency exchange hacked for $150 million
- Louis Vuitton fixes data leak and account takeover vulnerability
- Microsoft Advanced Compliance Solutions in Zero Trust Architecture
- All four of the world's largest shipping companies have now been hit by cyber-attacks
- Red Team — Automation or Simulation?
- ESET discovers a rare APT that stayed undetected for nine years
- Serious Security: Phishing without links – when phishers bring along their own web pages
- Cyber Security Awareness Month is here!
- With API attacks rising, Cloudflare launches a free API security tool
- Account takeover fraud rates skyrocketed 282% over last year
- GitHub rolls out new Code Scanning security feature to all users

#Patch Time!

- Critical Flaws Discovered in Popular Industrial Remote Access Systems
- NVIDIA fixes high severity flaws in Windows display driver
- Microsoft Issues Updated Patching Directions for 'Zerologon'
- Cisco Issues Patches For 2 High-Severity IOS XR Flaws Under Active Attacks
- Over 247K Exchange servers unpatched for actively exploited flaw

#Tech and #Tools

- The Powerful HTTP Request Smuggling
- CertAlert: Get warned when a certificate is due to expire
- Graphology of an Exploit – Hunting for exploits by looking for the author's fingerprints
- GHunt: OSINT tool to extract informations Google Account email.
- AttackerKB: short description and value/ease of use assessment of new CVEs
- Hacking Punkbuster
- Trasa: Open Source Identity Aware proxy
- Salesforce Policy Deviation Checker
- OWASP APICheck: DevSecOps toolset for HTTP APIs
- Updates to Ghostwriter: UI and Operation Logs

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us