MUST READ: Test and Trace program skipped GDPR privacy assessment

Microsoft takes control of 99 domains operated by Iranian state hackers

Microsoft takes control of 99 domains operated by APT35/Phosphorus cyber-espionage group.

By Catalin Cimpanu for Zero Day | March 27, 2019 -- 18:04 GMT (11:04 PDT) | Topic: Security

November 1, 2017 - Redmond, Washington: Microsoft's sign and flags of United States, Washington and Microsoft are visible in front of a building at company's corporate headquarters

/ Getty Images

Court documents (https://noticeofpleadings.com/phosphorus/) unsealed today revealed that Microsoft has been waging a secret battle against a group of Iranian government-sponsored hackers.

SECURITY

SigRed: A 17-year-old 'wormable' vulnerability for hijacking Microsoft Windows Server (https://www.zdnet.com/article/critical-sigred-vulnerability-impacts-microsoft-windows-dns-2003-2019-patch-now/)

The real reason Apple is warning users about MacBook camera covers (https://www.zdnet.com/article/the-real-reason-apple-is-warning-users-about-macbook-camera-covers/)

Best security keys in 2020: Hardware-based two-factor authentication for online protection (https://www.zdnet.com/article/best-security-keys/)

Best password managers for business in 2020: 1Password, Keeper, LastPass, and more (https://www.zdnet.com/article/best-password-managers/)

Cyber security 101: Protect your privacy from hackers, spies, and the government (https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/)

Hacking healthcare: Why medical devices, hospitals are tempting targets (ZDNet YouTube) (https://www.youtube.com/watch?v=3f8uatXJIRM)

Top 6 cheap home security devices in 2020 (CNET) (https://www.cnet.com/how-to/top-cheap-home-security-devices-in-2020-amazon-echo-smart-cam-wyze/?ftag=CMG-01-10aaa1b)

Why organizations shouldn't automatically give in to ransomware demands (TechRepublic) (https://www.techrepublic.com/article/why-organizations-shouldnt-automatically-give-in-to-ransomware-demands/?ftag=CMG-01-10aaa1b)

The OS maker sued and won a restraining order that allowed it to take control of 99 web domains that had been previously owned and operated by a group of Iranian hackers known in cyber-security circles as APT35, Phosphorus, Charming Kitten, and the Ajax Security Team.

The domains had been used as part of spear-phishing campaigns aimed at users in the US and across the world.

APT35 hackers had registered these domains to incorporate the names of well-known brands, such as Microsoft, Yahoo, and others. The domains were then used to collect login credentials for users the group had tricked into accessing their sites. The tactic is decades old but is still extremely successful at tricking users into unwittingly disclosing usernames and passwords, even today.

Some of the domains Microsoft has confiscated include the likes of outlook-verify.net, yahoo-verify.net, verification-live.com, and myaccount-services.net.

Microsoft said it received substantial support from the domain registrars, which transferred the domains over to Microsoft as soon as the company obtained a court order.

Companies often use court orders to take over domains that infringe on their trademark and copyrights. However, over the past year, Microsoft has been using this legal trickery to fight off hacker groups as well.

Further, this isn't the first time Microsoft has used a court order to take over domains that were previously under the control of government-backed cyber-espionage groups.

Over the 2018 summer, Microsoft also took control over domains operated by APT28 (https://www.zdnet.com/article/microsoft-weve-just-messed-up-russian-plans-to-attack-us-2018-midterm-elections/), a Russian cyber-espionage group also known as Strontium and Fancy Bear. Microsoft Corporate Vice President of Customer Security & Trust Tom Burt said today in a blog post (https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/) that they used this trick 15 times to take control of 91 domains operated by APT28, some of which were being used for campaigns aimed at the US 2018 midterm elections.

The practice of using court orders to take over malware domains isn't new, but until recently has only been used by US government agencies when they wanted to take over the command and control servers of malware botnets.

Recent cases include when the FBI used it to take control of the VPNFilter router malware (https://www.zdnet.com/article/fbi-to-all-router-users-reboot-now-to-neuter-russias-vpnfilter-malware/) last May, and when the DOJ used it in January this year to take control of Joanap (https://www.zdnet.com/article/doj-moves-to-take-down-joanap-botnet-operated-by-north-korean-state-hackers/), a botnet built by North Korean state hackers.

These were 2017's biggest hacks, leaks, and... (/pictures/biggest-hacks-leaks-and-data-breaches-2017/)

SEE FULL GALLERY (/pictures/biggest-hacks-leaks-and-data-breaches-2017/)

(/pictures/biggest-hacks-leaks-and-data-breaches-2017/) (/pictures/biggest-hacks-leaks-and-data-breaches-2017/2/) (/pictures/biggest-hacks-leaks-and-data-breaches-2017/3/) (/pictures/biggest-hacks-leaks-and-data-breaches-2017/4/) (/pictures/biggest-hacl leaks-and-data-breaches-2017/5/)

1 - 5 of 28 NEXT > ()

RELATED MALWARE AND CYBERCRIME COVERAGE:

- Police Federation hit by ransomware attack (https://www.zdnet.com/article/police-federation-hit-by-ransomware-attack/)
- North Korean hackers continue attacks on cryptocurrency businesses (https://www.zdnet.com/article/north-korean-hackers-continue-attacks-on-cryptocurrency-businesses/)
- Lithuanian man pleads guilty to scamming Google and Facebook out of $123 million (https://www.zdnet.com/article/lithuanian-man-pleads-guilty-to-scamming-google-and-facebook-out-of-123-million/)
- Hackers abuse Magento PayPal integration to test validity of stolen cards (https://www.zdnet.com/article/hackers-abuse-magento-paypal-integration-to-test-validity-of-stolen-credit-cards/)
- LockerGoga bug crashes ransomware before encrypting files (https://www.zdnet.com/article/lockergoga-bug-crashes-ransomware-before-encrypting-files/)
- Top dark web marketplace will shut down next month (https://www.zdnet.com/article/top-dark-web-marketplace-will-shut-down-next-month/)
- How the United Nations helps fight global cybercrime (https://www.techrepublic.com/article/how-the-united-nations-helps-fight-global-cybercrime/) TechRepublic
- Google blocked 2.3 billion bad ads in 2018 (https://www.cnet.com/news/google-blocked-2-3-billion-bad-ads-for-tickets-garage-doors-tech-support-in-2018/) CNET

RELATED TOPICS: MICROSOFT SECURITY TV DATA MANAGEMENT CXO DATA CENTERS

By Catalin Cimpanu for Zero Day | March 27, 2019 -- 18:04 GMT (11:04 PDT) | Topic: Security

SHOW COMMENTS

MORE RESOURCES