


As we move closer to the end of the year, it is important to remember that the threat actors do not take off for the holidays. Looking back through this week's good, bad and the ugly will help to understand the state of the technology landscape. Starting with the good, we score a few wins for the good guys by both Interpol and the FBI. Moving to the bad with a massive haul by the bad guys and wrapping up with the ugly involving both another zero-day as well as the feared zero-click vulnerabilities are discovered.

Starting with the conclusion of a 30-month long investigation from Interpol, spanning different continents, the take down of the CIOp ransomware gang is a big win. The gang targeted companies in the US and Korea as well as others by blocking access to files and systems and then demanding payment to restore the access. The investigation resulted in the search of more than 20 locations and seizing \$185,000 in cash assets. Looking closer to home, the FBI was able to seize the darknet site from the Blackcat ransomware gang. While the threat actors are fighting back and attempting to regain control of the marketplace, it does still appear to be displaying the FBI splash page. Blackcat is suspected to be behind the ransom of the MGM systems and have affected at least 1000 victims. Providing a RaaS offering, the gang would rent out or sell exploits to accomplish these attacks.

Although these are big wins for the good guys, we cannot forget that the bad guys are still working hard. With the successful theft of \$53 Million from 63k people, the crypto drainer uses ads on Google and Twitter to push malicious ads out. The tactic uses a phishing suite to drain the funds from Crypto accounts and can be purchased for a \$1,500 fee plus 20% of funds stolen with it. Like most legitimate software, the suite has additional feature add-ons that can be added for an additional \$500-1000. X, formerly known as twitter, is reported to have 6 out of 9 ads that are phishing ads.

Finally, we look at the ugly. While threat actors are always looking for the next new exploit and companies work to close these as fast as possible, it is important to remember that this is an ongoing battle. With Google patching its 8th zero-day of the year. This helps highlight the fact that patching is a never-ending process. Unfortunately



these zero-days tend to come from the well-funded, state-sponsored threat groups and are usually found to be actively exploited in the wild. The exploit threat actors use spyware to target the victims to include politicians, government officials and journalists. Adding to the ugly is the zero-click flaw within Outlook. By using calendar invites, threat actors are able to gain a foothold into systems without any user intervention. As you can imagine, these are the most detrimental as they are accomplished without the need for interaction on the side of the user. This bypass is a bypass to a patch put in place earlier this year. Threat analysis groups have determined that the attack vector was being actively used in attack from the APT28 group known as Forest Blizzard. This is a Russian back threat group. The attackers were able to use the exploits to take over victim exchange accounts. As of now, the suggested mitigation is to use micro segmentation to block outgoing SMB connections to remote public IPs.

Keeping an eye on the cat and mouse game between threat actors and law enforcement can make for interesting reads, as long as you are not the target of the mouse of course. Whether it is the win for the good guys or a win for the bad, knowing how attackers are targeting victims and knowing when the good guys are able to get remediation for attacks is important in knowing the landscape of the world of Cyber. Finally, knowing how to mitigate attacks, be it patching or knowing if other steps need to be taken is the first line in defending against the threats.

Thank you,

Caleb Leggett

