On October 13, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla, Google, Apache, Microsoft, Apple, and Adobe products.
See Latest CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
15 Oct	240,388,930	4,897,401

Deaths this week: 48,749

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN
15 October 2021

In The News This Week

CryptoRom Scam Rakes in $1.4M by Exploiting Apple Enterprise Features

The campaign, which uses the Apple Developer Program and Enterprise Signatures to get past Apple's app review process, remains active. - Pyramid-scheme cryptocurrency scammers are exploiting Apple's Enterprise Developer Program to get bogus trading apps onto their marks' iPhones. So far, so good: They've made off with at least $1.4 million in ill-gotten gains so far. That's according to Sophos Labs, which observed the scam making the rounds on dating sites. "They strike up a friendship, using the dating game as a ruse, but then quickly move to money, this time in the guise of them doing you a big favor by offering you a chance to join an 'unbeatable' investment opportunity," researchers said in a Wednesday posting. That investment opportunity involves cryptocurrency trading, with the offer to invest money into cryptocoins in order to reap big profits. To lend a veneer of legitimacy, the crooks offer an "official" iPhone app, purportedly approved by Apple.
Read the full story by Tara Seals here: ThreatPost

New Yanluowang ransomware used in targeted enterprise attacks

A new and still under development ransomware strain is being used in highly targeted attacks against enterprise entities as Broadcom's Symantec Threat Hunter Team discovered. The malware, dubbed Yanluowang ransomware (after a Chinese deity Yanluo Wang, one of the ten kings of hell) based on the extension it adds to encrypted files on compromised systems. It was recently spotted while investigating an incident involving a high-profile organization after detecting suspicious activity involving the legitimate AdFind command line Active Directory query tool. AdFind is commonly used by ransomware operators for reconnaissance tasks including gaining access to information needed for lateral movement through their victims' networks.
Read the full story here: Bleeping Computer

Once-in-a-decade discovery made

OTTAWA, ON, Oct. 14, 2021 /PRNewswire/ - Field Effect, a global cyber security company, has released details of their discovery of seven 0-day vulnerabilities in Microsoft Windows software and operating systems. The six privilege escalations and one info leak put billions of Windows users at risk. Dubbed collectively as "Blackswan" by Field Effect due to the unexpected find, the quantity, and the detection challenge, these bugs have amazingly existed **in Windows since the 2007 release of Windows Vista**. Such an extensive discovery is extremely rare, and Field Effect estimates that nearly every Windows computer in the world is vulnerable if unpatched, potentially impacting businesses worldwide. Matt Holland, Founder, CEO, and CTO of Field Effect, says all seven of these vulnerabilities add to a perfect attack scenario and would be easy to utilize as part of a ransomware or nation-state attack chain against businesses of any size and type. In its Patch Tuesday updates on July 13, 2021 and September 14, 2021, Microsoft issued patches for the first vulnerability, CVE-2021-34514, and the next five vulnerabilities, including CVE-2021-38628, CVE-2021-38629, and CVE-2021-38638. Patches for the seventh vulnerability CVE-2021-26442 were released on October 12, 2021. Read the full story here: PR Newswire

This 'relentless' malware botnet has made millions with a surprisingly simple trick

Malware researchers reckon this botnet has made millions by exploiting an easy shortcut taken by many. - The long-running botnet known as MyKings is still in business and has raked in at least $24.7 million by using its network of compromised computers to mine for cryptocurrencies. MyKings, also known as Smominru and Hexmen, is the world's largest botnet dedicated to mining cryptocurrencies by free-riding off its victims desktop and server CPUs. It's a lucrative business that gained attention in 2017 after infecting more than half a million Windows computers to mine about $2.3 million of Monero in a month. Security firm Avast has now confirmed its operators have acquired at least $24.7 million in various cryptocurrencies that have been transferred to Bitcoin, Ethereum and Dogecoin accounts. It contends, however, that the group made most of this through its 'clipboard stealer module'. When it detects that someone has copied a cryptocurrency wallet address (for example to make a payment) this module then swaps in a different cryptocurrency address controlled by the gang.
Read the full story by Liam Tung here: ZDNet

A Close Look at Russia's Ghostwriter Campaign

By now most of us will recognise the fact that the world is gripped in various campaigns of digital warfare. And as we look back at the "Cold War" that supposedly ended in the late '80s, the actors didn't change much. However, with the rapid and expansive development of technology and the interconnected world, the methods changed drastically and the stage is firmly set for digital warfare. With all that said, Karim Hijazi and Matt Stafford published a piece in Darkreading this week taking a closer look at the Russian Ghostwriter group and today I want to share a brief extract of the article, just to give you an idea of what is happening out there. For the full story, please visit the Darkreading site.

Overview - Russia's online disinformation efforts are vast and growing. While most of the US media's attention to date has focused on Moscow's efforts in the US elections, this overlooks an even more robust campaign that has been underway in Europe for quite some time. Known as "Ghostwriter," this espionage and disinformation operation has targeted several European countries, including Germany, Poland, Ukraine, and the Baltics (Estonia, Latvia, and Lithuania). In September, both Germany and the European Union officially attributed recent, targeted phishing campaigns to Russia generally and Russia's military intelligence apparatus (GRU) and the Ghostwriter operation specifically. In August, our intelligence team uncovered new operational details for Ghostwriter/UNC1151, which we publicly released on Sept. 1.

Ghostwriter's Infrastructure Is Significantly Larger Than Previously Thought - We identified an additional 81 phishing domains associated with UNC1151 that were not previously reported, which makes this group's infrastructure nearly three times larger than originally suspected. Of these new domains, 52 are assessed with high confidence to be part of UNC1151's operational infrastructure, and 29 are assessed with moderate confidence to be previously used phishing infrastructure for the actor's targeted phishing campaigns.

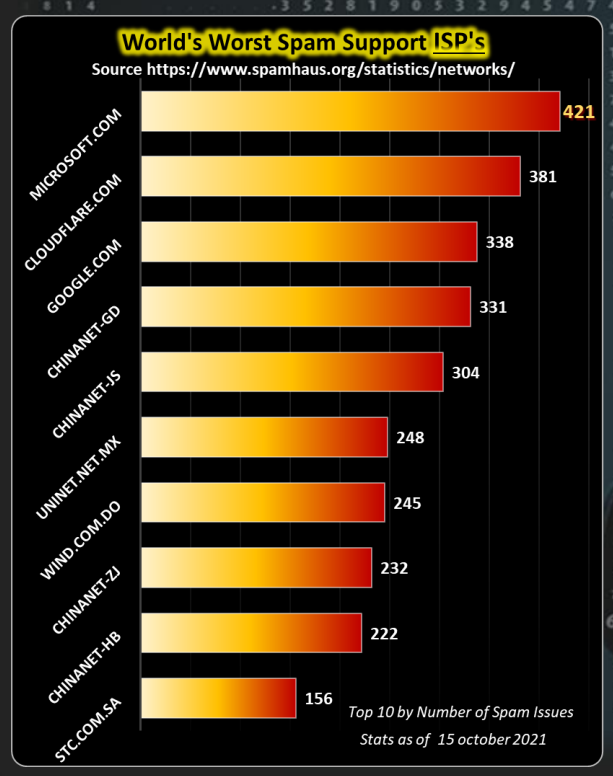
This Infrastructure Was Well Hidden - There were no overt linkages between the new domains our team discovered and the previous domains reported by Mandiant. The group used entirely different, and largely legitimate-looking registration information, login IPs, etc. It also did not follow the standard practice among criminal groups of registering new domains but instead re-registered older, expired domains with prior records and established histories (in some cases, these domains were 10 years old) in order to skew analysis and appear legitimate. Many of the domains were still inactive, which suggests the threat actor anticipated some level of domain attrition and had prepared for it by establishing backups.

Shifting Tactics - Our team also discovered domain and subdomain naming themes that indicate a change in Ghostwriter's targeting around 2020/2021. Consistent subdomain and root domain naming themes strongly reinforce our assessment that the target audience in 2019 and 2020 was Apple (iPhone and iCloud) users in Europe; nearly all root domains we identified have at least one subdomain that includes the words "apple" or "icloud." We also observed phishing subdomains that appear to target PayPal and OVH Telecom (a French web hosting and cloud computing company) accounts, as well as Google, Microsoft, Twitter, and Facebook. The evidence shows that in late 2020 and early 2021, the actor began a shift in targeting as indicated by the choice of specific subdomains attached to the generic root domain: UNC1151 began using subdomains that appear to target an Eastern European audience. It is during this time that we see a large-scale phishing infrastructure built out to phish credentials across the user spectrum: official Polish government accounts; Ukrainian military accounts; the French Armed Forces' Defense Information and Communication Delegation; accounts for popular regional email providers, such as Yandex, meta[.]ua, and bigmir[.]net; and global tech giants, including Twitter, Facebook, and Google.

Broader Range of Targets - As noted above, UNC1151's malicious campaign has expanded (and is likely still expanding) its geographical range to new targets.

The Bigger Picture - It's no small feat for a threat actor to hide this level of infrastructure from the types of experienced security teams and researchers who have been investigating it over the past two years. This suggests the Ghostwriter operation is much more sophisticated than was previously thought. Additionally, the cost of setting up this level of infrastructure — from the domain registrations to the VPNs and proxies needed to conceal these operations — isn't trivial, particularly when one considers that the campaign isn't intended to make money. All of this reinforces the attribution of state sponsorship made by Germany and the EU.

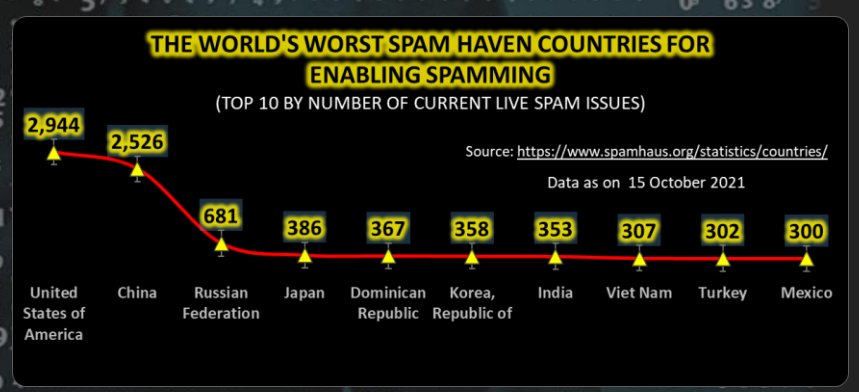
Ghostwriter's Future - These newly uncovered domains have shed more light on Ghostwriter's tactics, techniques, and procedures (TTPs), which will make it easier for organizations to identify and counteract future efforts by the group. However, UNC1151 has had its infrastructure published and disseminated in public reporting before and has been observed both moving to new infrastructure as well as continuing to use known, previously disclosed infrastructure. If publishing its infrastructure does, indeed, lead to diminishing operational effectiveness, we may see the group go silent, possibly to re-emerge later under a different banner, utilizing different TTPs and targeting methodologies, or perhaps not. This actor has been conducting a long-running, large-scale, and geographically dispersed influence operation for years and its operations and targets have evolved during that time. Its goals are not defined by the group or its members, but the strategic mission with which it is tasked — conducting espionage and spreading disinformation. Once these operations have achieved their objective or exposure has degraded their ability to operate, the group may jettison infrastructure, disband, reconstitute, retool, or develop new TTPs to avoid detection.
We may see Ghostwriter change its domain registration services, or use separate cloud infrastructure to host the SMTP servers for its phishing emails. It may even pivot from a focus on credential phishing via email to social media or other vectors.
Russia's disinformation efforts in Europe will go on, but whether it will continue to use the Ghostwriter operation remains to be seen. Either way, security teams should expect significant changes in the tactics used by this actor.



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Other Interesting News and Cyber Security bits:

- Anatomy of a cyber attack (Podcast)
- Lessons from a cyber-security breach
- Google unveils new security programs
- Anglo American launches pioneering North cyber-security apprenticeship scheme



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com