Your Security Rabbits report for February 15, 2022

Hot topics

Nothing today

News

Cyware News - Latest Cyber News

'Cities: Skylines' Gaming Modder Banned Over Hidden Malware
The modder, who goes by the handle Chaos as well as Holy Water, reportedly tucked an automatic updater into several mods that enabled the author to deliver malware to anybody who downloaded them.

Threatpost

'Cities: Skylines' Gaming Modder Banned Over Hidden Malware
35K+ players were exposed to an auto-updater that planted a trojan that choked performance for fellow modders and Colossal Order employees.

Naked Security

Adobe fixes zero-day exploit in e-commerce code: update now!
There's a remote code execution hole in Adobe e-commerce products - and cybercrooks are already exploiting it.

Threatpost

Adobe: Zero-Day Magento 2 RCE Bug Under Active Attack
The vendor issued an emergency fix on Sunday, and eCommerce websites should update ASAP to avoid Magecart card-skimming attacks and other problems.

Cyware News - Latest Cyber News

Asian Cloud Service Providers Face Threats from CoinStomp Cryptominer
Researchers have uncovered a cryptojacking malware named CoinStomp that is targeting Asian cloud service providers. To prevent forensic actions against itself, the malware tries to tamper with Linux server cryptographic policies. The use of such techniques indicates that attackers are aware of incident response systems and are trying to gain immunity to it.

Security Affairs

BlackByte ransomware breached at least 3 US critical infrastructure organizations
The US Federal Bureau of Investigation (FBI) said that the BlackByte ransomware gang has breached at least three organizations from US critical infrastructure sectors. The US Federal Bureau of Investigation (FBI) published a joint cybersecurity advisory with the US Secret Services which revealed that the BlackByte ransomware group has breached at least three organizations from US critical [...] The post BlackByte ransomware breached at least 3 US critical infrastructure organizations appeared first on Security Affairs.

Threatpost

BlackByte Tackles the SF 49ers & US Critical Infrastructure
Hours before the Superbowl and two days after the FBI warned about the ransomware gang, BlackByte leaked what are purportedly the NFL team's files.

IT Security Guru

Croatian phone carrier reports data breach
'A1 Hrvatska', a Croatian phone carrier, has disclosed a data breach exposing the personal information of roughly 200,000 of its customers. The organisation has not provided many details outside the fact that they suffered a cybersecurity incident involving the unauthorised access of one of their user databases containing sensitive personal information. The information leaked includes [...] The post Croatian phone carrier reports data breach appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Data of 1.2 Million Guests of Harbour Plaza Hotels in Hong Kong Impacted by Cyberattack
Hong Kong's privacy watchdog said on Friday that it had received reports from the firm two days ago about a cybersecurity incident involving several databases for room reservations.

Cyware News - Latest Cyber News

Dissecting the ModifiedElephant APT Group and its Campaign
Researchers uncovered a decade-old APT, dubbed ModifiedElephant, that has been delivering multiple malware on the systems of human rights activists and defenders, academics, and lawyers in India. Moreover, it uses spear-phishing emails to spread keyloggers, RATs such as NetWire, DarkComet, and several Android malware strains. Like this, there could be more such groups operating from under the shadows and undetected right now.

Security Affairs

European Central Bank tells banks to step up defences against nation-state attacks
The European Central Bank is warning banks of possible Russia-linked cyber attack amid the rising crisis with Ukraine. The European Central Bank is warning banks of possible Russia-linked cyber attack amid the rising crisis with Ukraine and is inviting them to step up defenses. The news was reported by Reuters, citing two unnamed sources. The [...] The post European Central Bank tells banks to step up defences against nation-state attacks appeared first on Security Affairs.

The Hacker News

Experts Warn of Hacking Group Targeting Aviation and Defense Sectors
Entities in the aviation, aerospace, transportation, manufacturing, and defense industries have been targeted by a persistent threat group since at least 2017 as part of a string of spear-phishing campaigns mounted to deliver a variety of remote access trojans (RATs) on compromised systems. The use of commodity malware such as AsyncRAT and NetWire, among others, has led enterprise security firm

CyberScoop

For signs of cryptocurrency laundering, look closely at Moscow firms, report says
Moscow-based businesses appear to be handling much of the money laundering of cryptocurrency payments that come from global ransomware activity and other forms of cybercrime, according to a report from crypto-tracking company Chainalysis. The analysts focused on several dozen companies with a presence in Moscow City, the Russian capital's skyscraper-packed business district. In any given quarter, "illicit and risky" blockchain addresses account for between 29% and 48% of all funds received by those cryptocurrency businesses, the report says. That traffic, including legitimate crypto transactions, can sometimes be more than $1 billion in a quarter, Chainalysis says. "A huge amount of cryptocu[...]

WeLiveSecurity

From the back office to the till: Cybersecurity challenges facing global retailers
How well retailers can manage the surge in cyberthreats may be crucial for their prospects in a post-pandemic world The post From the back office to the till: Cybersecurity challenges facing global retailers appeared first on WeLiveSecurity

Cyware News - Latest Cyber News

Google Chrome emergency update fixes zero-day exploited in attacks
The zero-day bug fixed today, tracked as CVE-2022-0609, is described as a "Use after free in Animation" and was assigned a High severity level. It was found by a researcher from Threat Analysis Group.

Security Affairs

Google fixes a Chrome zero-day flaw actively exploited in attacks
Google fixed a high-severity zero-day flaw actively exploited with the release of Chrome emergency update for Windows, Mac, and Linux. Google fixed a high-severity zero-day flaw, tracked as CVE-2022-0609, actively exploited with the release of Chrome emergency update for Windows, Mac, and Linux. This is the first Chome zero-day fixed this year by Google. The zero-day [...] The post Google fixes a Chrome zero-day flaw actively exploited in attacks appeared first on Security Affairs.

IT Security Guru

Google update fixes zero-day vulnerability

Google has released Chrome 98.0.4758.102 for Windows, Mac, and Linux, as fix for a high-severity zero-day vulnerability used by cyber-attackers. "Google is aware of reports that an exploit for CVE-2022-0609 exists in the wild," the company said in a security advisory released today. Chrome update will roll out over the coming weeks but it is possible [...] The post Google update fixes zero-day vulnerability appeared first on IT Security Guru.

Cyware News - Latest Cyber News

KlaySwap Cryptocurrency Users Lose Funds After Clever BGP Hijack

The attack took place earlier this month, on February 3, lasted only for two hours, and KLAYswap has confirmed the incident last week and is currently issuing compensation for affected users.

IT Security Guru

Major car dealer suffers ransomware attack

Emil Frey, a Swiss car dealer have released a statement confirming that they were hit with a ransomware attack last month. The company, which is ranked as the number 1 car dealership in Europe, showed up on the list of victims for the Hive ransomware on February 1 later confirming that they were attacked in [...] The post Major car dealer suffers ransomware attack appeared first on IT Security Guru.

IT Security Guru

Morley companies suffers data breach

A data breach at a business services company based in Saginaw, Michigan may have exposed the personal information of 521,00 people. The attack was detected on August 1 last year when data in the company's care became unavailable. The breach comes as a direct result of cyber-criminals targeting Morley Companies. Michigan attorney general Dana Nessel confirmed [...] The post Morley companies suffers data breach appeared first on IT Security Guru.

The Hacker News

New MyloBot Malware Variant Sends Sextortion Emails Demanding $2,732 in Bitcoin

A new version of the MyloBot malware has been observed to deploy malicious payloads that are being used to send sextortion emails demanding victims to pay $2,732 in digital currency. MyloBot, first detected in 2018, is known to feature an array of sophisticated anti-debugging capabilities and propagation techniques to rope infected machines into a botnet, not to mention remove traces of other

Cyware News - Latest Cyber News

OilRig's New Marlin Backdoor and the Group's Lyceum Connection

OilRig APT's activity has been spotted in its new Out to Sea campaign that introduces a new backdoor, dubbed Marlin, and targets organizations in the Middle East. Marlin uses Microsoft's OneDrive API for its C2 operations, which shows that the group quit its traditional use of DNS and HTTPS for C2 communications. Furthermore, researchers have linked OilRig's activities to the Iranian cybercriminal group known as Lyceum owing to numerous TTPs overlaps.

Naked Security

Power company pays out $3 trillion compensation to astonished customer

More money than the UK's economy produces in a year!

Security Affairs

Remote sex toys might spice up your love life - but crooks could also get a kick out of them

A CyberNews investigation has revealed that Lovense remote sex toy users might be at risk from threat actors, due to poor security features. Original post: https://cybernews.com/privacy/remote-sex-toys-might-spice-up-your-love-life-but-crooks-could-also-get-a-kick-out-of-them/ Lovense boasts that its teledildonic sex toys will spice up your sexual relationship. By using wireless remote control, you can customize vibrations and adjust them to your body, or [...] The post Remote sex toys might spice up your love life - but crooks could also get a kick out of them appeared first on Security Affairs.

IT Security Guru

Scammers increasingly targeting women on dating sites

TSB has released data ahead of Valentine's day showing how dating sites are "riddled with scammers". Unfortunately, it has shown that women were targeted in two-thirds of the cases it analysed and the average age of those scammed was 47 years old. The average amount of money swindled from women was PS6,300 compared with men [...] The post Scammers increasingly targeting women on dating sites appeared first on IT Security Guru.

Security Affairs

SSU: Russia-linked actors are targeting Ukraine with 'massive wave of hybrid warfare'

The Security Service of Ukraine (SSU) said the country is the target of an ongoing "wave of hybrid warfare." The Security Service of Ukraine (SSU) today revealed the country is the target of an ongoing "wave of hybrid warfare" conducted by Russia-linked malicious actors. Threat actors aim at destabilizing the social contest in the country [...] The post SSU: Russia-linked actors are targeting Ukraine with 'massive wave of hybrid warfare' appeared first on Security Affairs.

Cyware News - Latest Cyber News

The rise of the super malicious insider: Yes, we need to worry

The super malicious insider accounted for 32% of malicious insider incidents investigated in 2021. DTEX Systems also noted a 72% year-over-year increase in actionable insider threat incidents.

IT Security Guru

Half of all emails in 2021 were spam

Email spam rates averaged 46% over the year globally, according to a new report by Kaspersky. In its new Spam and Phishing in 2021 report, the Russian AV company revealed that spam rates peaked at 48% in June. The majority came from machines in Russia (25%), followed by Germany (14%), the US (10%) and China (9%). [...] The post Half of all emails in 2021 were spam appeared first on IT Security Guru.

IT Security Guru

Local authority earmarks $380k for cyber-attack recovery

Following a breach in December, Gloucester City Council has set aside $380k to recover from the incident. The local authority admitted at the time of the attack that it could take up to 6 months fix as servers would need rebuilding. Councillors have admitted, however, that the sum may not be enough to handle the [...] The post Local authority earmarks $380k for cyber-attack recovery appeared first on IT Security Guru.

Cyware News - Latest Cyber News

More Than 500,000 Addresses Leaked from NSW Government Database

The hundreds of thousands of locations were collected by the NSW Customer Services Department through its QR code registration system and made public through a government website.

The Hacker News

New Chrome 0-Day Bug Under Active Attack - Update Your Browser ASAP!

Google on Monday rolled out fixes for eight security issues in the Chrome web browser, including a high-severity vulnerability that's being actively exploited in real-world attacks, marking the first zero-day patched by the internet giant in 2022. The shortcoming, tracked CVE-2022-0609, is described as a use-after-free vulnerability in the Animation component that, if successfully exploited,

Cyware News - Latest Cyber News

NFT Lure Used to Distribute BitRAT

In an attempt to hide stolen information, this variant of BitRAT stores collected data (keystrokes, clipboard data, etc.) in an alternate data stream (ADS) file that is majority encoded in Base64.

IT Security Guru

One Identity launches Cloud Infrastructure Entitlement Management

One Identity, the provider of unified identity security, has announced the availability of One Identity Cloud Infrastructure Entitlement Management (CIEM), enabling businesses to support governance and privileged access for cloud infrastructure objects. The company said this innovation along with other new releases such as its Application Governance module and a new connector to Microsoft Teams, [...] The post One Identity launches Cloud Infrastructure Entitlement Management appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Ransomware Becomes Deadlier, Conti Makes the Most Money

Ransomware actors are constantly upgrading their TTPs and finding new ways to make profits. A new report by Chainalysis states that ransomware victims spent almost $700 million in ransom in 2020.

Blog â€" Flashpoint

Russia Is Cracking Down on Cybercrime. Here Are the Law Enforcement Bodies Leading the Way.

Recent takedowns lead to arrests On February 7 and 8, the domains of several well-known Russian-language illicit communities--Ferum Shop, Sky-Fraud, Trump Dumps, and UAS--were seized by Department K, a division of the Ministry of Internal Affairs of the Russian Federation that focuses primarily on information technology-related crimes. In addition to seizing the domains, Russian authorities [...] The post Russia Is Cracking Down on Cybercrime. Here Are the Law Enforcement Bodies Leading the Way. appeared first on Flashpoint.

IT Security Guru

Sensitive business addresses published in COVID data breach

The addresses of defence sites, a missile maintenance unit and domestic violence shelters were among the 500,000 addresses leaked by mistake. This is the first major breach of the New South Wales government's huge store of QR code data. Premier Dominic Perrottet said the information was uploaded in error and "shouldn't have happened". The mistake [...] The post Sensitive business addresses published in COVID data breach appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Team Xecuter hacker gets 40 months in prison for Nintendo Switch hacks

Team Xecuter is a group of hackers operating for over a decade. The gang is mainly involved in developing devices and software to hack Nintendo consoles like 3DS and the Switch.

Cyware News - Latest Cyber News

TrickBot Uses Metaprogramming in BazarBackdoor Malware

In a new twist, authors of BazarLoader and BazarBackdoor malware were spotted utilizing template-based metaprogramming to obfuscate important data. Researchers found similar code patterns in malware samples as is found when samples are built using ADVobfuscator, an obfuscation library based on C++11/14 and metaprogramming. For protection, a better understanding of these techniques may help malware reverse engineers to create more efficient tools for analysis.

IT Security Guru

Ukraine says it has been targeted by Russian cyber-attacks

The Security Service of Ukraine (SSU) says that the attacks aim provoke anxiety and undermine Ukrainian society's confidence in the state's ability to defend its citizens. "Ukraine is facing attempts to systemically sow panic, spread fake information and distort the real state of affairs. All this combined is nothing more than another massive wave of [...] The post Ukraine says it has been targeted by Russian cyber-attacks appeared first on IT Security Guru.

Krebs on Security

Wazawaka Goes Waka Waka

In January, KrebsOnSecurity examined clues left behind by "Wazawaka," the hacker handle chosen by a major ransomware criminal in the Russian-speaking cybercrime scene. Wazawaka has since "lost his mind" according to his erstwhile colleagues, creating a Twitter account to drop exploit code for a widely-used virtual private networking (VPN) appliance, and publishing bizarre selfie videos taunting security researchers and journalists. In last month's story, we explored clues that led from Wazawaka's multitude of monikers, email addresses, and passwords to a 30-something father in Abakan, Russia named Mikhail Pavlovich Matveev. This post concerns itself with the other half of Wazawa[...]

CyberScoop

Years of hacks against aviation, transportation industries are tied to one group, researchers say

Analysts have noticed various attempts in recent years by hackers trying to breach entities in the aviation and aerospace industries, as well as related transportation fields. The operators typically use of off-the-shelf malware and deploy digital lures that refer to industry-specific topics like airline cargo conferences or machine parts. It now appears that most of those incidents were by the same group, according to cybersecurity firm Proofpoint. Dubbing the group "TA2541," Proofpoint says the trail of evidence goes back to at least 2017, and the hackers remain a "consistent, active cybercrime threat." Hundreds of different organizations have been targeted globally, with an emphasis on No[...]

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

CVE-2021-24839

The **SupportCandy WordPress** plugin before 2.2.5 does not have authorisation and CSRF checks in its wpsc_tickets AJAX action, which could allow unauthenticated users to call it and delete arbitrary tickets via the set_delete_permanently_bulk_ticket setting_action. Other actions may be affected as well.

HIGH Vector: network Created: 2022-02-07 Updated: 2022-02-15

Source: Hybrid Analysis

Top malicious files

100% Threat score	FH-1503757750 (.) xlsb	100% Threat score	typedesk 1 (.) 2 (.) 0 (.) exe
100% Threat score	d148562a49a09333b2b02d13e12b183d4c3fcf23fbb024d4e0b440631a3a3663	100% Threat score	RR (.) exe
100% Threat score	NumKey (.) exe	100% Threat score	dc627b6419366cdf50eccfa3d1995c111b71112e5abb725b6096b9e0026af395
100% Threat score	bfb2a7f8e7396f8edee131eca9715ab8b2fc957478b7cf0d58840a707b718e09	100% Threat score	b7730f9a05be8a0f25a3979b2f8d2fed791340a32385a9fd37d0e8b81119627d
100% Threat score	a713a2749e9791243a89471a2603bf1f32ec11c9179771ca46fb5583b8412cb0	100% Threat score	a60f5b41251d0bf126fc3c2b836de7d59aa608fd6d37726d71960dd408575512
100% Threat score	75972d15f3b2e97d52b9f8a6f42ea85976ed5bb9d609c3bf93ee98d6f4f4a648	100% Threat score	233ee2ea02322d3da68217ab4b51722a4a3aa833667a45377dfd4742d5979c4c
100% Threat score	wwaaaaalllllaaaa (.) exe	100% Threat score	clop (.) bin
100% Threat score	pdf_payload-HA2 (.) pdf	100% Threat score	itools_Setup_Release_prod_11 (.) 54_signed (.) exe
100% Threat score	e05ab504ac650f4946bf9242fc528c25bc17a9654705cc51a6fb6a11ad8641bc (.) exe	100% Threat score	e05ab504ac650f4946bf9242fc528c25bc17a9654705cc51a6fb6a11ad8641bc (.) exe
93% Threat score	d3bb736d8a8b500c75ad853392afac37fd8cd519b274db4cba9451d2f1899059	85% Threat score	disksavvy_setup_v14 (.) 1 (.) 16_x64 (.) exe
85% Threat score	OnVUE-3 (.) 78 (.) 106 (.) exe	80% Threat score	Efax-Inv32847-MT (.) htm
77% Threat score	c2sehbbiqkiqcffnj (.) exe		

Source: Hybrid Analysis

Top malicious URL

95% Threat score	http://nen-tomonokai (.) co (.) jp/journal (.) html#test%40test (.) com
84% Threat score	http://sportstream (.) tv/
82% Threat score	http://nomiswap (.) io/
79% Threat score	https://86vb02idu3 (.) s3 (.) us-south (.) objectstorage (.) softlayer (.) net/fon/index (.) html?key=b4191a7c82f7d6bf34373f0f4f53f494&redirect=https%3A%2F%2Fwww (.) amazon (.) com#spedycja (.) legnica%40gls-poland (.) com
77% Threat score	http://www (.) dancarbon (.) com/
77% Threat score	http://www (.) thebestorganization (.) com/
77% Threat score	http://www (.) wohomen (.) com/
77% Threat score	http://www (.) plefora (.) co (.) uk/
77% Threat score	http://ttiquabo (.) sysnetsoft (.) com/
72% Threat score	http://www (.) jerrycala (.) com/
72% Threat score	http://morganstanley (.) monster/
72% Threat score	http://217 (.) 182 (.) 232 (.) 206/movistarplus (.) exe
72% Threat score	http://www (.) calamillor (.) guru/

Source: SpamHaus

Top spamming countries

#1 United States of America	#2 China
#3 Russian Federation	#4 Mexico
#5 Dominican Republic	#6 Saudi Arabia
#7 India	#8 Japan
#9 Brazil	#10 Korea, Republic of

Source: SpamHaus

Top spammers

#1 **Canadian Pharmacy**
A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting.

#2 **PredictLabs / Sphere Digital**
This operation uses dozens of "hosting" companies as fronts to lease IP addresses which are then used to send spam. Based in Chicago, Illinois and Tangier, Morocco.

#3 **Hosting Response / Michael Boehm**
Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IP addresses and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates.

#4 **Mint Global Marketing / Adgenics / Cabo Networks**
Florida affiliate spammers and bulletproof spam hosters

#5 **RetroCubes**
Web development, application development, and business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.

#6 **Michael Persaud**
Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.

#7 **Cyber World Internet Services/ e-Insites**
Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox. The company is owned or managed by Alvin Slocombe.

#8 **RR Media**
A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.

#9 **Kobeni Solutions**
High volume snowshoe spam operation based in Florida. The manager or owner of the company seems to be a Yair Shalev / . (Former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO-listed spammer Dan Abramovich. Sued for fraud by the US FTC in 2014.

Source: SpamHaus

Top countries with botnet

#1 China	#2 India
#3 United States of America	#4 Thailand

#5 Indonesia	#6 Algeria
#7 Viet Nam	#8 Brazil
#9 Iran (Islamic Republic of)	#10 Pakistan

Source: SpamHaus

Top phishing countries

#1 United States	#2 Germany
#3 Russia	#4 Netherlands
#5 United Kingdom	#6 Hong Kong
#7 Canada	#8 Singapore
#9 France	#10 Australia