Cyber Digest

Mobcast on Security Trends & Threats

November 2024

Volume I

CYBERai COMMUNE

RansomHub gang allegedly behind attack on Mexican airport operator

A hacking group recently spotlighted by U.S. agencies said it is responsible for an attack targeting an operator of 13 airports across Mexico. Full Story

Four REvil Ransomware Members Sentenced in Rare Russian Cybercrime Convictions

Marking one of the rare instances where cybercriminals from the country have been convicted of hacking and money laundering charges. Full Story

Landmark Admin Says 800K Affected In Data Breach

One of the biggest third-party administrators for several large insurance firms said a cyberattack in May exposed the sensitive information of more than 800,000 people. Full Story

China Is Scanning Canada’s Cyber Defenses, State Watchdog Warns

The Canadian government warned that “a sophisticated state-sponsored threat actor from the People’s Republic of China” has been scanning the cyber defenses of important public entities. Full Story

Chinese Hackers Are Said to Have Targeted Phones Used by Trump and Vance

Chinese hackers targeted data from phones used by former President Donald J. Trump and his running mate, Senator JD Vance of Ohio, as part of what appears to be a wide-ranging intelligence-collection effort. Full Story

Iranian hackers have probed US election websites for vulnerabilities

Iranian government-linked hackers have researched and probed election-related websites in multiple U.S. swing states, in a possible effort to discover vulnerabilities that could be used to influence the presidential election. Full Story

LinkedIn Fined More Than $300 Million in Ireland Over Personal Data Processing

Ireland's data-protection watchdog fined LinkedIn 310 million euros ($334.3 million), saying the Microsoft-owned career platform's personal-data processing breached strict European Union data-privacy and security legislation. Full Story

Pokémon Developer Game Freak Hacked; Decades of Data Leaked

Game Freak, the Japanese video game developer behind the Pokémon franchise, has been hit by a massive data breach, now being referred to as the "Teraleak." Full Story

Five Sentenced in Austria's Largest Crypto Scam of $21.6M

Five individuals in Austria have been sentenced for their involvement in a staggering $21.6 million cryptocurrency fraud scheme that defrauded around 40,000 investors. Full Story

Hackers are extorting Globe Life with stolen customer data

Insurance giant Globe Life is being extorted by a hacker that has stolen customers' sensitive data. Globe Life says that approximately 5,000 individuals are known to be affected by the breach so far, but the number is likely to be far higher. Full Story

Ransomware gang stoops to new low, targets prominent nonprofit for disabled people

A notorious ransomware gang previously responsible for attacks on multiple hospitals has now claimed a new victim: disability nonprofit Easterseals. Full Story

Brazil arrests USDoD hacker tied to FBI, National Public Data breaches

The Department of Federal Police (DPF) has arrested a 33-year-old hacker from Belo Horizonte (MG), believed to be responsible for some of the most significant global cyberattacks on critical infrastructure. Full Story

Fortifying Your Organization: Essential Cyber Security Tips and Best Practices

Block Hash SHA 256

IOC	Threat Category	TI* Reputation	TI* Score
7c11773cb1e4e197628838d5372c315bebb463d53cb490fcc130b6a2d4b92898	Malware (Trojan)	-	-
40228faee1c9b862483968af6312243ddfd111251b7422acfa7be64bda544878	Adware	Malicious	76
71226b69696e60a14e516c80e0852e636e9c2ac1f4498eeb8d38d4a93dc57391	Adware	-	-
564b8e327a13c948cea21587245b7b0005f786ea57f62bd602ef4ecec66171c6	Adware	Malicious	77
7c5710a667583384267c949471f2a4388f5081808352dd1ec1d585e3cacd5811	Malware (Trojan)	Suspicious	25
c22c7dd3a9ce14e576a1f7d853e1302849236c8aa61c0b38b40016ead581a408	Adware	Malicious	65
77200156d4773175d341aad11ab23bd52445065cd95060348da17d083dc27688	Adware	Malicious	72
833064195b0c96bce9a8c00dc95df6bd9fce1092c1260ba0e877810bfc44b0aa	Malware (Trojan)	Malicious	72
058f6ca087ddd809a525c4f47444c42669ae83eda91eba2d05abc5a5553fd564	Malware (Trojan)	Malicious	77
3c0bd30009f4c97bb96742dbb873efc062a111bf6f4a39b808471310628bb42d	Malware (Trojan)	Malicious	75

*TI : Threat Intelligence

Domain

IOC	Threat Category	TI* Reputation	TI* Score
jburke@dcmstl.com	Phishing	-	-
a.bullerwell@stcuthbertsk.org	Phishing	-	-
hermiklosfmer.invoicinglawyer.com	Phishing	-	-
lvx.com.ar	Phishing	Suspicious	25

IPv4 Address

IOC	Threat Category	TI* Reputation	TI* Score
46.246.34.52	Brute Force	-	44
46.246.34.53	Brute Force	Unusual	10
46.246.34.54	Brute Force	Unusual	10
46.246.34.29	Brute Force	Unusual	5
89.208.104.19	Brute Force	Unusual	15
45.151.99.150	Brute Force	Suspicious	36
45.151.99.154	Brute Force	Unusual	10