QUALYSEC
BEYOND CYBERSECURITY

2023
MARCH 2ND WEEK

CYBER SECURITY NEWS

CONTACT US

www.qualysec.com
865 866 3664
contact@qualysec.com

Police Seized Website Selling Malware Used to Hack Computers

Federal investigators in Los Angeles confiscated an internet site used to sell computer malware used by hackers to grab control of affected systems and steal a variety of information.

“A RAT is a type of malware that allows for covert surveillance, allowing a ‘backdoor’ for administrative control and unfettered and unauthorized remote access to a victim’s computer, without the victim’s knowledge or permission”, based on court records submitted in Los Angeles.

Swiss Law Enforcement Seized Control of the Computer Server

Croatian officials arrested a citizen who was supposedly the website’s administrator. The Croatian government will bring charges against this offender.

Also, the server hosting the NetWire RAT infrastructure was also taken by Swiss law enforcement.

Reports stated that in 2020, the only known online distributor of NetWire, worldwidelabs, was the subject of an investigation by the FBI in Los Angeles. Additionally, the software was promoted on hacking forums, and numerous cybersecurity firms and governmental organizations have documented instances of the NetWireRAT being used in criminal activity.

Source : https://cybersecuritynews.com/police-seized-website-malware/?amp

Hackers Exploiting Remote Desktop Program Flaws to Install PlugX Malware

ASEC (AhnLab Security Emergency response Center) has recently reported that in order to deploy PlugX malware, threat actors are exploiting vulnerabilities in Chinese remote desktop programs like:-

- Sunlogin
- AweSun

The use of these flaws on compromised systems continues to be exploited to deliver a variety of payloads as a result of ongoing abuses. The following are included:-

- Sliver post-exploitation framework
- XMRig cryptocurrency miner
- Gh0st RAT
- Paradise ransomware

There are a number of malware on this list, but PlugX is the most recent. Chinese threat actors have extensively used modular malware, with new features constantly being added to aid in the theft of sensitive information and control of systems.

Moreover, there is a possibility that an attacker can gain control over an infected system by installing PlugX without the user knowing. It is consequently possible for a variety of malicious behavior to be perpetrated as a result of this.

Source : https://cybersecuritynews.com/install-plugx-malware/?amp

Bitwarden Password Manager Flaw Let Attackers Steal User's Credentials

The Flashpoint Vulnerability Research team observed that Bitwarden, a well-known password manager browser extension, treated embedded iframes on web pages in an unusual way.

The <iframe> HTML element defines a nested browsing environment, embedding another HTML page into the current one, according to the Mozilla HTML documentation.

Bitwarden first became aware of the issue in 2018 but decided to support it in order to support legitimate websites that employ iframes.

Auto-Fill Behavior in Bitwarden

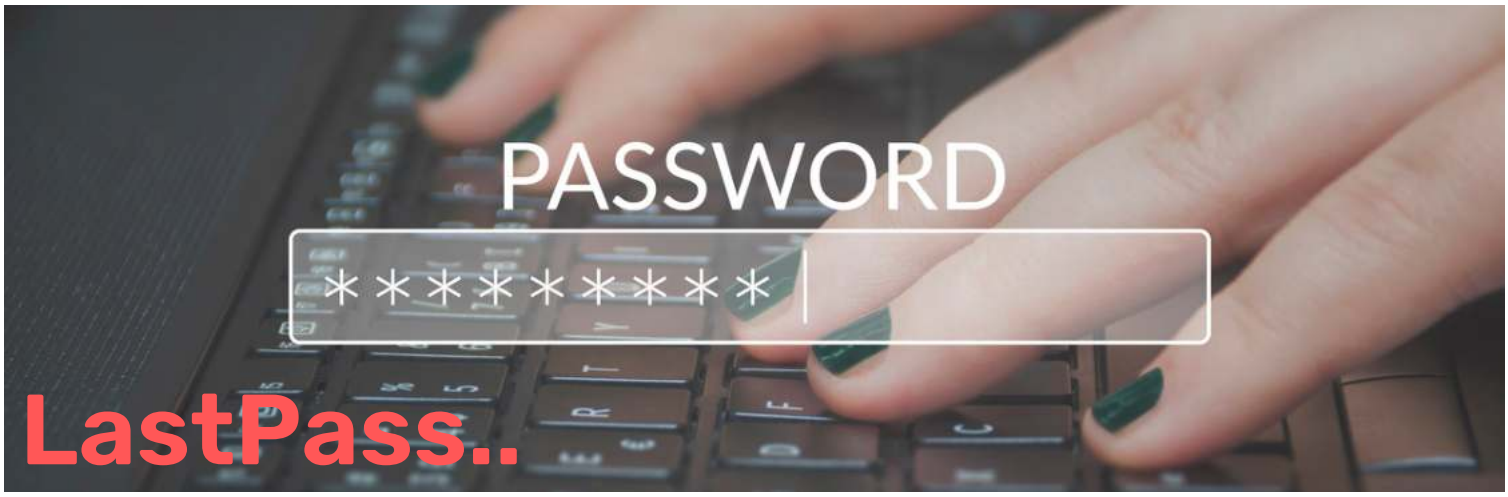
The Bitwarden extension can offer to fill in the appropriate login fields when it recognizes that a user is on a website for which they have saved credentials.

Potential Attack Methods

- An unhacked website with the "Auto-fill on page load" option turned on embeds an external iframe that is in the hands of an attacker.
- Using a subdomain of, say, a hosting company, which has its login form under the same base domain, an attacker installs a specially crafted web page.

In response, Bitwarden stated that they would not change the functionality of iframes but would promise to block autofill on the reported hosting environment in a future release.

Source :https://cybersecuritynews.com/bitwarden-password-manager-flaw/?amp



LastPass Massive Hack Tied to Engineer Failure to Update Plex on Home Computer

One of LastPass's engineer neglected to update Plex on their personal computer, which led to the company's significant breach. Plex claims that the vulnerability is almost three years old and has been fixed for a very long time.

To install malware on the LastPass employee's home computer, the hacker chose the Plex Media Server software as his target.

Facts of the Massive Data Breach Brought On By Engineers Not Updating the Plex Software

The company officially informed users of the vulnerability, tracked as CVE-2020-5741, (CVSS score: 7.2) in May 2020. A deserialization bug hitting Plex Media Server for Windows allows a remote, authenticated attacker to execute arbitrary Python code in the context of the current operating system user.

The hacker used keylogging malware that was installed on the user's home computer to "capture the employee's master password as it was entered, after the employee authenticated with MFA (multi-factor authentication), and gain access to the DevOps engineer's LastPass corporate vault," according to LastPass.

Source : https://cybersecuritynews.com/lastpass-massive-hack/?amp

Acer Hacked – Over 160GB of Data for Sale on Hacking Forum

Acer, a global Taiwanese company that makes hardware and electronics, has admitted that one of its servers was compromised. Attackers broke into document servers used by repair technicians and stole 160GB of data, which was then sold.

Yet according to the company, the findings of its preliminary inquiry do not show that this security problem has affected consumer data.

More Than 160GB of Data Are Offered For Sale

The Bleeping Computer report says that the data breach has been confirmed after a threat actor who claims to have stolen data from Acer in mid-February 2023 started selling it on a well-known hacking forum.

Particularly, the threat actors released screenshots of technical schematics for the Acer V206HQL display, documents, BIOS definitions, and confidential files as evidence that they had stolen data.The data poster stated that they were selling the complete dataset to the highest bidder and clarified that they would only take payment in hard-to-trace cryptocurrency Monero (XMR).

Hence, always take precautions to safeguard your sensitive data and systems, including using strong passwords, enabling multi-factor authentication, updating your software and firmware, and keeping an eye out for any unusual behavior.

Source : https://cybersecuritynews.com/acer-hacked/?amp

Beware! Hackers Abusing Public Cloud Infrastructure to Host DBatLoader Malware

Recently, several phishing campaigns have been identified by the security analysts at SentinelOne using the DBatLoader malware loader that distributes the Remcos RAT. As far as their target is concerned, they are targeting Eastern European businesses and institutions primarily.

DBatLoader makes use of the public cloud infrastructure as a way to host its malware staging component in order to facilitate its operations. A variety of forms and methods are used by threat actors to distribute RAT through phishing emails.

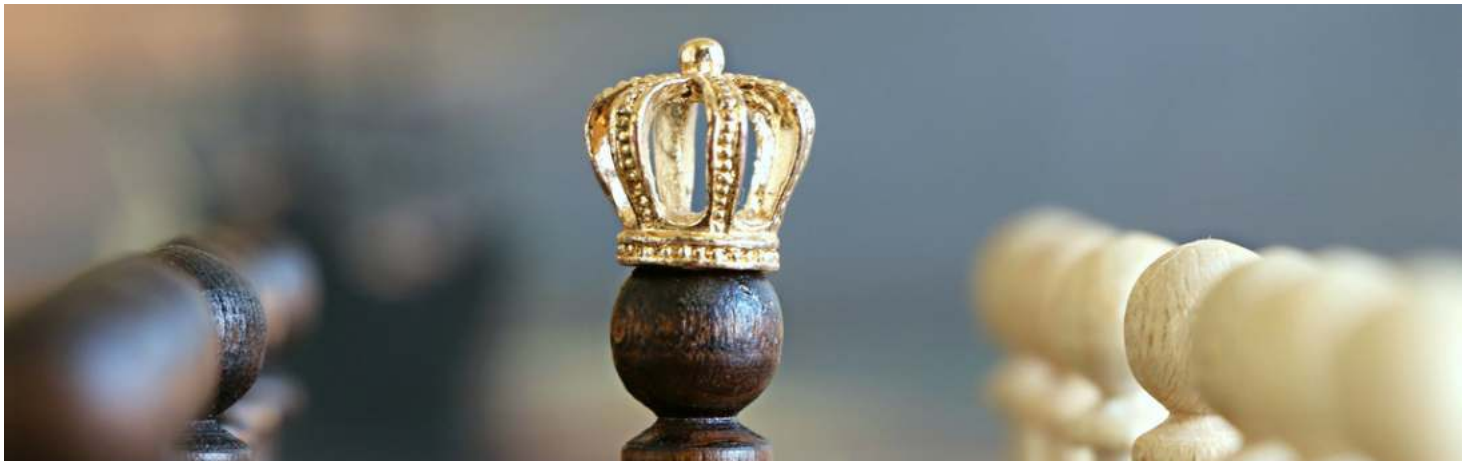
Using password-protected archives as email attachments, Remcos RAT phishing campaigns targeted Ukrainian state institutions. While these institutions are targeted for the purpose of conducting espionage operations.

Spreading via Phishing Emails

The “tar.lz” archive attachments are included in phishing emails that distribute DBatLoader and Remcos. Most of the time, these attachments are disguised as financial documents like:-

- Invoices
- Documents related to tenders

Source : https://cybersecuritynews.com/hackers-abusing-public-cloud-infrastructure/?amp



Royal Ransomware Made Upto $11 Million USD Using Custom-Made Encryption Malware

The collaborative efforts of the FBI and CISA have resulted in the creation and distribution of a comprehensive Cybersecurity Advisory (CSA) revealing that the threat actors behind the Rayal ransomware made up to $11 million in Crypto.

This advisory has been designed to share crucial information on the Royal ransomware threat and its associated IOCs and TTPs.

The FBI's dedicated threat response activities have identified these IOCs and TTPs recently in January 2023, and the CSA aims to share this information to help organizations protect themselves against this malicious threat.

A new variant of Royal ransomware has been used by cybercriminals to breach the security of both US-based and foreign organizations since around September 2022.

The FBI and CISA believe that the custom-built file encryption program utilized by a particular ransomware variant is an evolved version of previous iterations that employed a loader known as "Zeon." Recent reports indicate that Royal ransomware has advanced its capabilities and can now target both Windows and Linux environments. This suggests that the attackers are adapting and evolving their tactics to expand the scope of their attacks.

Source : https://cybersecuritynews.com/royal-ransomware/?amp

“It is crucial for users to exercise caution when receiving spam emails or to visit phishing websites and to verify the source before downloading any applications”, concludes the researchers.

It's a fact that cybercrime is on the rise and it's more important than ever to protect your business from cyber threats.

But the good news is that you don't have to navigate the complex world of cybersecurity alone. Our team of experts is here to help you cyber security testing services need to protect your application or business.

Don't wait for a cyber attack to happen. Contact us now to learn more about how we can help secure your business and give you peace of mind.

Contact now and protect your business with our expert cyber security services.

CONTACT US AT