Weekly Intelligence Trends/Advisory

20 May 2022

TABLE OF CONTENTS

1. CYFIRMA's Weekly Insights **[NEW]**

1.1 Weekly Attack Type and Trends

Key Intelligence Signals:

- **Attack Type:** Malware Implant, Ransomware, Vulnerabilities & Exploits, Ransomware-as-a-Service (RaaS), Data Leak, Cyber Espionage, Spear-phishing, Data Exfiltration, Persistence, Account Takeover, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Remote Code Execution (RCE), OS Command Injection
- **Objective:** Data Theft, Payload Delivery, Data Encryption, Financial Gains, Unauthorized Access, Espionage
- **Business Impact:** Data Loss, Financial Loss, Reputational Damage, Operational Disruption
- **Ransomware – LockBit (LockBit 2.0)| Malware – RedLine Stealer**
  - **LockBit –** One of the ransomware groups.

  Please refer to the trending malware advisory for details on the following:
  - Malware – **RedLine Stealer**

  Behavior - Most of these malware use phishing and social engineering techniques as their initial attack vector. Apart from these techniques, exploitation of vulnerabilities, defence evasion, and persistence tactics are being observed.

1.2 Threat Actor in Focus

Sidewinder APT' Two-year Attack Spree Across Asia

Suspected Threat Actors: SideWinder

- **Attack Type:** Cyber Espionage, Spear-phishing, Data Exfiltration, Vulnerabilities & Exploits, Persistence, Malware Implant
- **Objective**: Espionage, Unauthorized Access, Potential Data Theft
- **Target Technology**: Email, Windows, Android
- **Target Industry**: Military, Law enforcement, Foreign Affairs, Defense, Aviation, IT, and Legal Institutions, Government
- **Target Geography**: South Asia, Central Asia
- **Business Impact**: Data Loss

Summary: During the Black Hat Asia conference, a security researcher detailed a two-year-long campaign conducted by an advanced persistent threat gang known as **SideWinder** which they have been tracking since 2017. The APT group has conducted approximately 1,000 raids and leveraged complex and increasingly sophisticated attack methods including multiple layers of malware, additional obfuscation, and memory-resident malware that leaves researchers little evidence to work on.

The main initial access vector of this threat actor group consists of spear-phishing emails with malware-laced attachments that are targeted toward a curated list of targets. The group does not leverage Zero-days exploits, but instead makes use of known Windows or Android vulnerabilities.

While the initial research showed SideWinder being linked to India, however, over the years the attribution of this threat actor has become a challenge.

Insights:

- The researcher highlighted that SideWinder APT stands apart from other APT groups due to its large toolset that includes many different malware families, various new spear-phishing documents, and a very large infrastructure. In addition, SideWinder showcases dogged persistence and a high volume of activity.
- The group has also been found to be switching gears if the first attack attempt fails to infiltrate the victim. They remain careful and innovative while approaching targets and ensure that they gain a foothold. In such an instance, the threat actor group sent out a spearphishing email that had a malicious payload, although no email content. After a short while, another spearphishing email containing an apology letter for the previous email was sent, however this time a different malicious payload was inside the document. All this was done to ensure that they got a foothold into the victim's environment.

1.3 Major Geopolitical Developments in Cybersecurity

Killnet Hackers Announce Cyberattacks on Countries Opposing Putin's War

A group of pro-Russian hackers who go by the name "Killnet", have announced that they "declare war" and intend to launch global cyberattacks against 10 countries including the UK – for standing up to Vladimir Putin's war in Ukraine.

The other countries mentioned as a target by the Russian-linked groups include the US, Germany, Italy, Latvia, Romania, Lithuania, Estonia, Poland, and Ukraine.

The development comes after Killnet's failed cyberattack against the Eurovision online voting system during the Eurovision Song Contest which was claimed to be disrupted by the Italian police. However, Killnet's announcement on Monday referred to it as false and called them the "deceitful police of Italy". In the same announcement, the Italian police were also featured in the target list in addition to 10 other countries mentioned above.

Killnet also claimed responsibility for the seemingly offline website of the cyber arm of the Italian police.

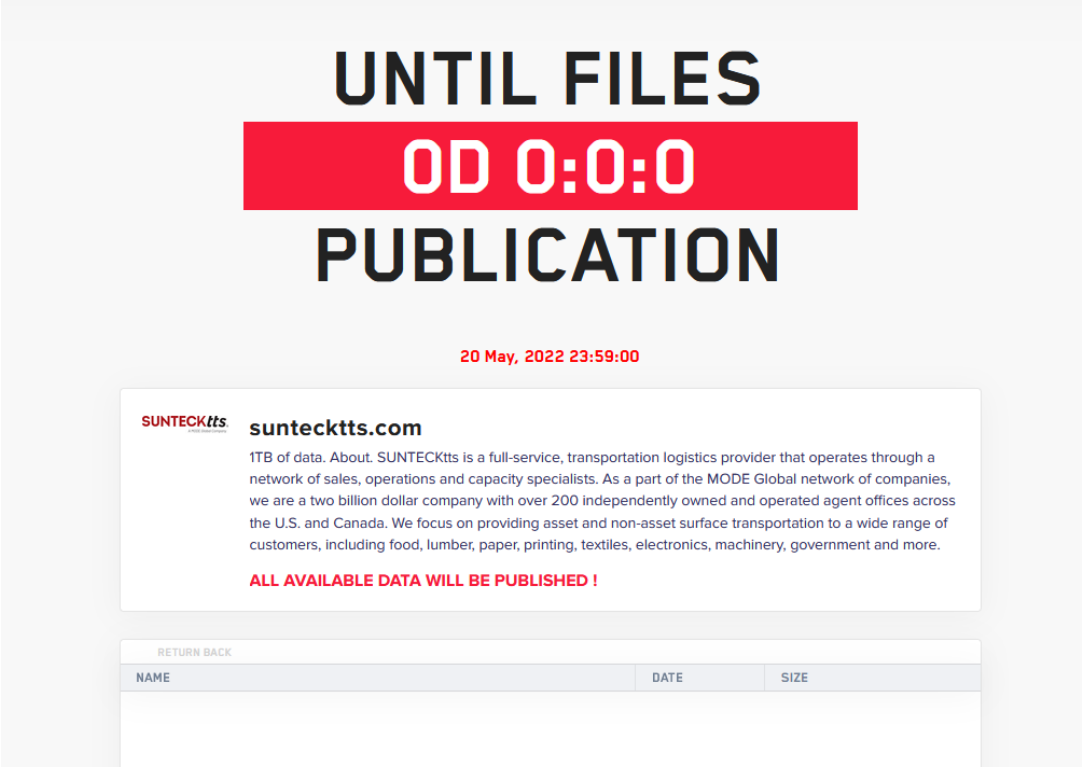
1.4 Rise in Malware/Ransomware and Phishing

SUNTECKtts Impacted by LockBit Ransomware

- **Attack Type**: Ransomware, Data Exfiltration
- **Target Industry:** Transportation, Logistics
- **Target Geography:** United States
- **Ransomware**: LockBit
- **Objective**: Data Theft, Data Encryption, Financial Gains
- **Business Impact**: Data Loss, Financial Loss, Reputational Damage

Summary: CTI observed **SUNTECKtts** – a **MODE Transportation** company that provides full-service multi-mode transportation solutions being impacted by the LockBit ransomware. The ransomware group had provided an update on their dedicated leaks site which claims **SUNTECKtts** as one of their victims. The ransomware group claims to have exfiltrated approximately 1 terabyte of company data. At the time of CTI's observation, no sample has been provided. It appears that the ransomware group is awaiting ransom negotiation and in case of non-compliance to their ransom demand, the group will likely publish all exfiltrated data on their dedicated leak site for anyone to download.

The following screenshot was observed published on the dark web:



Source: Dark Web

Insights:

- Around January 2020, LockBit operators first appeared on Russian-language cybercrime underground forums. In June 2021, the operators introduced version two of the LockBit RaaS, advertised as LockBit 2.0, and was reportedly bundled with StealBit – built-in information stealing function.
- The LockBit 2.0 operators are known to implement the double extortion techniques by threatening to publish the exfiltrated data to their dark web leak site "LockBit BLOG" if ransom demands are not met. The enforcement of such tactics coerces victims into paying the ransom demands.
- At the start of November 2021, the increased pressure from law enforcement agencies and the unavailability of members forced the prolific RaaS group BlackMatter to shut down its operations. However, researchers reported that existing BlackMatter affiliates are moving their victims to LockBit DLS – most likely to facilitate their extortion efforts. They observe that

the BlackMatter victims are provided with URLs to new negotiation pages which belong to LockBit. With more experienced affiliates joining the LockBit ransomware group, it is going to be one of the largest and arguably the most successful ransomware groups in operation.

- Alongside Conti, LockBit is one of the topmost prominent ransomware groups – with both groups accounting for nearly half of all ransomware attacks. Last month alone, LockBit ransomware had claimed more than 60 victims on their dedicated leak site with the majority of victims operating in US and European countries.

1.5 Latest Cyber-Attacks, Incidents, and Breaches

Bugs Chained to Takeover Facebook Accounts That Used Gmail

- **Attack Type**: Account Takeover, XSS, CSRF
- **Objective:** Unauthorized Access
- **Target Technology:** Facebook Accounts
- **Target Industry:** Social Media
- **Target Geography:** Global
- **Business Impact:** Data Loss, Reputational Damage

Summary: A security researcher has recently disclosed multiple bugs that he chained together to take over Facebook accounts linked to a Gmail account. The researcher who reported the issue to Facebook detailed each issue and steps to take over the account in his report which includes:

- **Sandboxed CAPTCHA –** The first issue was found in Facebook's extra security mechanism called "Checkpoint" which uses Google CAPTCHA presented in an iFrame hosted on a sandboxed domain (fbsbx.com). The "referrer" part in the URL for iFrame can be replaced with the "next" parameter by an attacker allowing them to send the URL including the login parameters to the sandbox domain.
- **XSS** – For testing purposes, Facebook makes it possible to upload custom HTML files that can be uploaded to their sandbox domain fbsbx.com.
- **SOP (Same Origin Policy)** – Since the same domain is in use for the Google CAPTCHA and where XSS is possible. This setup allows attackers to bypass the controls of the same origin policy since the target site and the custom script are on the same domain.
- **CSRF** – In the report, the researcher used undisclosed CRSF attacks to log the target user out and later log them back in through the Checkpoint.
- Next, an OAuth Access Token string is intercepted by targeting a third-party OAuth provider like Gmail.

Insights:

- The issue was reported to Facebook and reportedly has been fixed in February. Although the issue is the result of multiple bugs, the major bugs in the researcher's report are intended by design. This includes the XSS bug in the Facebook sandbox domain and another bug that enables sharing of sensitive information with this sandbox domain.
- As per the researcher, the exploitation was carried out only for Facebook users who signed up using a Gmail account which has an OAuth mechanism to authenticate users to Facebook. However, the researcher highlights that it was possible to target all Facebook users.

1.6 Vulnerabilities and Exploits

Researchers Warn of Hackers Targeting Zyxel Vulnerability

- **Attack Type:** Vulnerabilities & Exploits, RCE, OS Command Injection
- **Target Technology:** Zyxel Firewalls
- **Vulnerability:** CVE-2022-30525 (CVSS base score: 9.8)
- **Vulnerability Type:** Command Injection

Summary: Several researchers including NSA are warning about the widespread critical vulnerability that affects Zyxel firewall product line models that are being exploited by hackers. Starting on May 13, one of the researchers reported seeing exploitation attempts. The vulnerability is a type of OS command injection vulnerability that affects Zyxel firewalls supporting Zero Touch Provisioning (ZTP), which includes the ATP series, VPN series, and the USG FLEX series. An attacker successfully able to exploit vulnerable systems affected by this vulnerability could modify specific files and then execute some OS commands on a vulnerable device.

Insights:

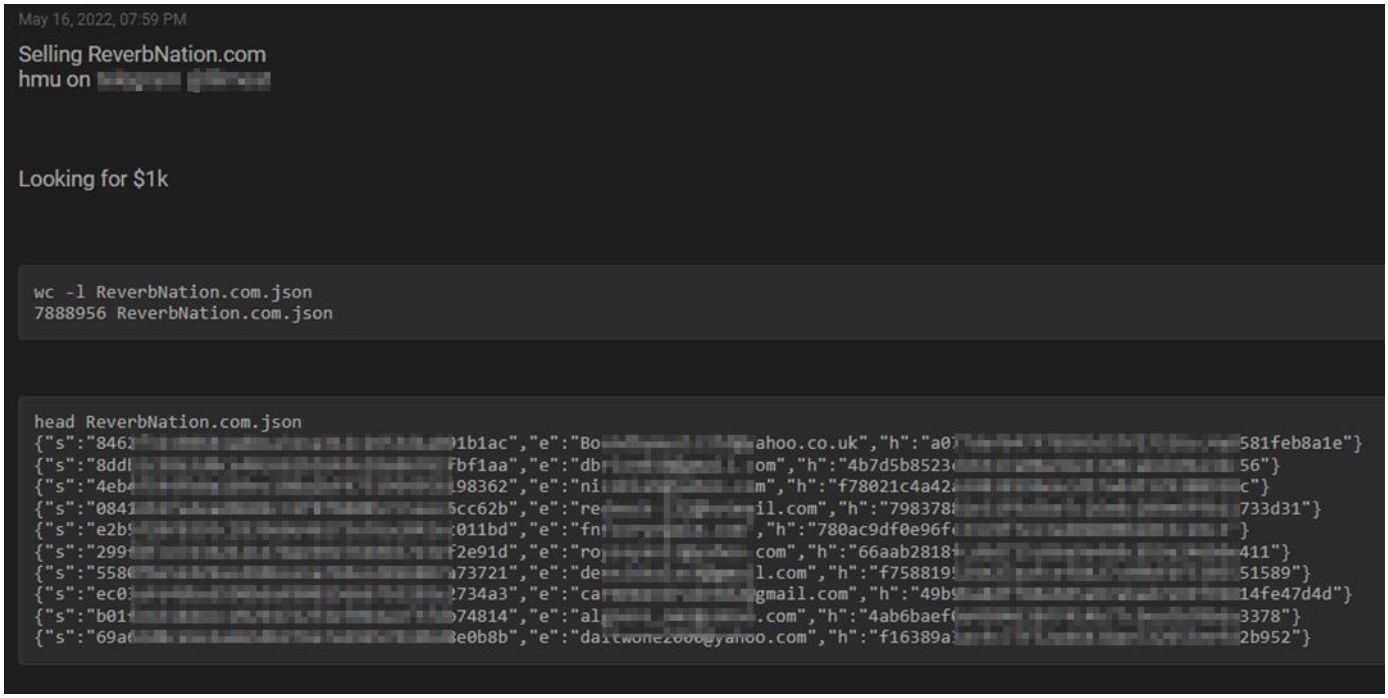
- After the disclosure, Zyxel patched the vulnerability in April, however, there were reports by various researchers of it being exploited in the wild. Researchers have seen approximately 20,800 Zyxel firewall models exposed over the internet that may be potentially affected by this vulnerability. The majority of such affected models reside in Europe - France (4.5K) and Italy (4.4K).
- The researcher who originally discovered and notified the issue to Zyxel had a fair amount of criticism on how the vulnerability was handled by the vendor. Without publishing an associated CVE, Zyxel patched the issue despite the researcher proposing a coordinated disclosure. The release of the patch is more or less similar to releasing details of the vulnerability and it is fairly trivial for attackers to reverse the patch and learn about the precise exploitation details.

1.7 Data Leak

ReverbNation Data Advertised for Sale

- **Attack Type:** Data Leak
- **Target Industry:** Media
- **Target Geography:** United States
- **Objective:** Data Theft, Financial Gains
- **Business Impact:** Data Loss, Financial Loss, Reputational Damage

Summary: As part of routine threat hunting efforts, CTI has observed potential data of **ReverbNation (reverbnation.com)** - which provides marketing services including networking and discovery tools features to the online music community across the world – leaked by an unknown threat actor in one of the underground forums. As per the advertisement, the threat actor claims to have secured access to approximately 7.8 million user records sold for USD 1000. From the sample records provided, the leaked data for sale includes emails address and SHA1 hash that may be related to users' passwords.



Source: Underground Forums

Insights:

- Opportunistic cybercriminals motivated by financial gains are always on the lookout for exposed and vulnerable systems and applications**.** The majority of these attackers operate in underground forums engaging in related conversations and buying/selling stolen digital goods. Unlike other financially motivated attackers such as ransomware groups or extortion groups who often publicize their attacks, these attackers like to operate under the hood. By taking advantage of an unpatched system or exploiting a vulnerability in an application or system – they gain access and steal valuable data. The stolen data is then advertised for sale in underground forums, resold, and repurposed by other attackers in their attacks.

2. Recommendations **[NEW]**

STRATEGIC RECOMMENDATIONS

Attack Surface Management should be adopted by organizations, ensuring that a continuous closed-loop process is created between attack surface monitoring and security testing.

Deploy a **unified threat management** strategy – including malware detection, deep learning neural networks, and anti-exploit technology – combined with vulnerability and risk mitigation processes.

Incorporate **Digital Risk Protection (DRP)** in the overall security posture that acts as a proactive defence against external threats targeting unsuspecting customers.

Implement a **holistic security strategy** that includes controls for attack surface reduction, effective patch management, active network monitoring, through next generation security solutions and ready to go incident response plan.

Create **risk-based vulnerability management** with deep knowledge about each asset. Assign a triaged risk score based on the type of vulnerability and criticality of the asset to help ensure that the most severe and dangerous vulnerabilities are dealt with first.

MANAGEMENT RECOMMENDATIONS

Take advantage of global **Cyber Intelligence** providing valuable insights on threat actor activity, detection, and mitigation techniques.

Proactively monitor **effectiveness of risk-based information security strategy**, the **security controls** applied and the proper implementation of **security technologies**, followed by corrective actions remediations and lessons learned.

Move beyond traditional model of security awareness towards **improved simulation and training** exercises that mimic real attack scenarios, account for behaviours that lead to a compromised and, are measured

Consider implementing **Network Traffic Analysis (NTA)** and **Network Detection and Response (NDR)** security system to compensate the shortcoming of EDR and SIEM solutions.

Detection processes are tested to ensure awareness of anomalous events. Timely communication of anomalies and continuously evolved to keep up with refined ransomware threats.

TACTICAL RECOMMENDATIONS

Patch software/applications as soon as updates are available. Where feasible, automated remediation should be deployed since vulnerabilities are one of the top attack vectors.

Consider using **security automation** to speed up threat detection, improved incident response, increased visibility of security metrics and rapid execution of security checklists.

Build and undertake safeguarding measures by monitoring/ blocking the IOCs and strengthen defences based on tactical intelligence provided

Deploy **detection technologies** that are behavioural anomaly-based to detect ransomware attacks and help to take appropriate measures.

Implement combination of security control such as **reCAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), Device fingerprinting, IP backlisting, Rate-limiting, and Account lockout** to thwart automated brute-force attacks.

Ensure **email and web content filtering** uses **real-time blocklists, reputation services** and other similar mechanism to avoid accepting content from known and potentially malicious sources.