Cyber Threat Intelligence insights

> *Who knows his enemy and himself, won't fear the result of a hundred battles*
>
> **Sun Tzu (544 – 496 av.JC)**

Cyber-Weather

Monthly News Roundup

April

sogeti
Part of Capgemini

Weak signals for Strategic CTI

IcedID and Qbot : growing access brokers for ransomware operations

In a coordinated joint operation led by EUROPOL, the **Emotet' infrastructure was disrupted on January, 27th 2021**. As "nature abhors a vacuum", other banking trojans like **IcedID** and **Qbot** seem to supersede as **privileged access brokers** to **eCrime groups** operating **ransomwares**.

The **Lunar Spider group** (see ecrime spotlight) is extending its pivotal role in the eCrime ecosystem: the development of its MaaS (Malware-as-a-Service) model opens up selling, or to sell the use of **IcedID**, to other groups seeking to gain a footprint on victims' network to eventually drop their ransomwares. **Lunar Spider** has reportedly added **Qbot** (aka **Qakbot**) to its arsenal, also playing the role of a ransomware dropper.

Qbot has previously been used in double-chain attacks allowing **Ryuk, Maze, Conti, Egregor and ProLock** infections. As IcedID does, **Qbot** allows post-exploitation operations downloading **Cobalt Strike** Beacons that could be used as command-and-control communications but also as additional payloads downloader.

IcedID leveraged as a first-stage infection already led to the ransomware deployment of **Maze, Egregor, Sodinokibi and RansomExx**. Moreover, strong connexions were spotted by researchers between **Lunar Spider** and **Wizard Spider** leading to sophisticated and harmful crime operations associating **IcedID** and **Trickbot** as loaders, owned respectively. Other links were spotted between **Sprite Spider** (the operators of the **Defray777 ransomware)** and **Lunar Spider**.

These loaders are most often based on the **same modus operandi**, *i.e.* poisoned attachments in mails. Recently, **both Qbot and IcedID** (or Gozi) has been observed leveraging a new trendy maldoc builder dubbed **EtterSilent** that allows attackers to craft fake DocuSign documents leveraging either **malicious Macros** or the **CVE-2017-8570** to download additional payloads on the victims' workstations.

It will be certainly more and more important to keep track on **Lunar Spider (IcedID), Mallard Spider (Qbot) and Bamboo Spider (Gozi) threat groups** that appears as "links cluster" especially when they leverage **EtterSilent** to empower their phishing operations and thus, with **high confidence**, sell previously obtained accesses to **ransomware groups**.

IcedID, Qbot, Lunar Spider, Wizard Spider, Bamboo Spider, Mallard Spider, Emotet, EtterSilent, Ransomwares

The eCrime ecosystem is **resilient**. The MaaS model on which **IcedID** and **Qbot** are based on, allows newcomers to the ransomware scene to **gain access to victim networks at a lower cost**

As **EtterSilent** continues to evolve, especially with more resilient **evasion techniques**, the latter is highly likely **to be increasingly used** in **phishing operations** that can lead **to impactful post-exploitation operations** (*i.e.*, CS, ransom/doxwares etc)

Cybercriminal groups' use of **loaders** such as IcedID and Qbot whose infection is facilitated by the maldoc builders EtterSilent can **lure detection teams focusing on ransomwares and not on banking trojans payloads**

The best (but also the most fragile) **defense against phishing remains the user**. **Regular Phishing simulations** on those type of threats and **awareness sessions** are highly **recommended**

Threat highlights

Natanz Iranian atomic site blackout allegedly resulted of a cyber attack by Israel

https://www.securityweek.com/iran-calls-natanz-atomic-site-blackout-nuclear-terrorism

This incident comes at a political time when the Islamic Republic of Iran and the state of Israel continue to threaten each other as the **Biden administration attempts to revive the Iran nuclear deal from which former U.S. President Donald Trump had withdrawn**.

As of writing, little information is available about the scope of the incident. However, the **possibility of a cyberattack that sought to cut off the power supply to part of the enrichment plants is the most likely**, according to several Israeli media outlets with reliable sources. If this hypothesis were to be confirmed, it could be a response by Israel to the various cyberattacks that occurred in 2020 against several water treatment plants, one of which was **aimed at modifying the level of chlorine** and thus posing a health security risk of national scope.

it is important to understand that Israel and Iran are two rival regional powers with robust offensive capabilities in cyberspace that can be mobilized to **support the two countries' respective foreign policies**. These cyber-state skirmishes are thus a way for the two states to gauge each other's strength and make "showdowns" in order to please the nationalists of both countries in their detestation of the traditional enemy.

It is highly likely that Iran will retaliate against Israel on this issue, especially by **increasing the targeting of APT groups on the Hebrew state and its regional allies**.

Natanz, Iran, Israel, Nuclear, Cyberattack, Retaliation

French hospital hit by a ransomware

https://www.databreaches.net/another-french-hospital-hit-by-cyberattack/

Beginning of **April**, a **French hospital** fell victim of a **ransomware** incident that led to the **disconnection of all workstations and servers to prevent lateralization**.

CERT Sogeti ESEC, in a coop with the **French security agency (ANSSI)** led investigations to evaluate the scope of the compromise and the remediations measures to take.
From the **ransom note content**, the **lack of data exfiltration / persistence** mechanisms and the use of **BestCrypt/Bitlocker** drawn the attribution towards **Timisoara Hacker Team ransomware** (aka **THT** is likely a Romanian-speaking threat actor as Timisoara is a Romanian city but also because Romanian comments were found in the ransomware source.
The **THT** group is **far from being well-known**, however researchers puzzlingly found the presence of **THT ransomware** evidence **within Hades** (**doxware) victim environment** (does not mean a link exists but it could).

HADES is supposedly the latest addition to the **Indrik Spider** (aka **Evil Corp**) eCrime group operating the infamous **Dridex** botnet.
Cybercriminals of **Evil Corp** have been recently tied to **the Russian government** by the **U.S. DEPARTMENT OF THE TREASURY. Hades** would be the **Indrik Spider's WastedLocker successor** as the latter was recently added to the blacklist of the U.S. Treasury Department's Office of Foreign Assets Control OFAC.

THT, Timisoara Hacker Team, Ransomware, Healthcare sector, France, HADES, Indrik Spider, Evil Corp, Dridex, WastedLocker

Latest Bab(u|y)k ransom|dox-ware TTPs

- For the CERT Sogeti ESEC, Babuk's developers are **Russian speaking** and are located in a **Central Asia** country, with a medium probability for **Kazakhstan** (thanks to SOCMINT-oriented research)
- Babuk being the name of a **slavic deimon**, we conjecture it could be the origin of the ransomware's name
- **13 victims have been hit this month** including the DC Police of Washington. The last victim's sensitive data have been removed from Babuk' dedicated leak site that suggests that negotiations are undergoing (confidential files are still available online if one knows where to look)

- As **we anticipated in the Cyber-weather of February** other groups such as **Babuk extended its capabilities of encryption** beyond Windows environment towards **virtualized critical systems (ESXi** in the same vein as Darkside and RansomExx) and **NAS**
  - **ESXi** : custom encryption scheme for virtual machines, hyperthreading with queue, log and statistics on completion to the console
  - **NAS** : QNAPP and Synology are supported, smudge encryption, log to console
- Babuk operators claim leveraging **entry vector as 0-days on:**
  - VPN servers (**TLP:AMBER** possibly FortiGate)
    -> With high probability
  - Proxylogon Microsoft Exchange Server (CVE-2021-26855)
    -> With Medium probability
  - RDP often used by small enterprises
    -> With Low probability

- Babuk operator(s) stated they will from now on **bypass the first extorsion scheme** (encrypting victim's data) **and focus on exfiltrating and doxing** instead (validates the Cyber-weather' anticipation of February)
- Their 'product' (as they call it) will be turned to an **Open Source Ransomware-as-a-service**
- They also seek to rent their infrastructure and brand to other groups deprived of dedicated leak sites.
- They published their public Tox chat ID to get offers for groups operating ransomwares.
- They also expressed their loyalty "to Dopplepaymer and Ragnar doxware" operators before removing this sentence in the final version... Again
- **Emsisoft reported** fundamental design **flaws** within both the **encrypting and decrypting** parts of Babuk **on ESXi**

- **Be prepared** : create, maintain and exercise a basic cyber incident response plan against ransomwares/doxwares
- Regularly test your backups; maintain them offline
  - In particular before using a decryptor
  - Maintain "gold images" of critical systems
- Apply our python **vaccine**
- **Focus efforts** of patching/monitoring **on your VPN servers**
  - use whitelists if possible / ban specific countries you are not interacting with
  - **Audit** the network for systems using **RDP**

sogeti
Part of Capgemini

Cyber-Weather
Spotlight

APT

Cozy Bear/APT29/The Dukes

Cozy Bear (aka APT29 or The Dukes) is an alleged Russian APT group suspected of being part of the Russian Foreign Intelligence Service (SVR). The victimology of Cozy Bear encompasses the Russian foreign policy and performs sophisticated cyberespionage operations mostly against Western countries.
In a White House official statement published on April, 15th 2021, the United States formally names **Cozy Bear as the perpetrator of the SolarWinds Orion supply-chain attack** occurred in December 2020. This attribution has led to a verbal and diplomatic escalation between Moscow and Washington that could lead to fears of new cyber operations more assumed by both countries.

Russia

- Nation state
- Political parties
- Software vendors
- Defense

- Solar Winds Orion supply-chain compromise
- Hammertoss RAT alleged developer

APT29, Cozy Bear, SVR, Solar Winds, USA, Russia, supply-chain

E-crime

Lunar Spider /TA551/ Shakthak

Lunar Spider (aka TA551 or Shakthak) is an alleged Russian speaking eCrime group operating **IcedID** (aka BokBot) and Valak malwares. Active from at least **2017**, Lunar Spider began its operations with banking trojans functionalities but in mid-2020 switched their strategy giving up Valak to exclusively distribute IcedID.
As such, Lunar Spider is allegedly **part of a cooperation ecosystem selling/offering its IcedID as a ransomware loader to other threat groups**. Lunar has organizational relations with Wizard Spider (Ryuk/Conti), Pinchy Spider (Revil), Sprite Spider (RansomEXX) and TA2101 (Maze/Egregor)

C.I.S

- Individuals
- Financial sector

- Mass phishing
- Password-protected attachments
- Ransomware loader

Lunar Spider, TA551, Shaktahk, Loader, Ransomware

Vulnerability

Increased exploitation of FortiOS vulnerabilities

The Federal Bureau of Investigation (**FBI**) and **CISA** have released a Joint Cybersecurity Advisory (CSA) to warn users and administrators that advanced persistent threat (APT) actors are actively exploiting known **Fortinet FortiOS** following vulnerabilities:

- **CVE-2018-13379**: A path traversal vulnerability in **FortiOS**
- **CVE-2020-12812**: Improper authentication vulnerability in **FortiOS SSL VPN**
- **CVE-2019-5591**: A default configuration vulnerability in **FortiOS**

Actors like **Cring** used these vulnerabilities to gain **initial access** to local services and, encrypted industrial sector companies' networks.

CVE-2018-13379, CVE-2020-12812, CVE-2019-5591, FortiOS, Cring, Crypt3r, Vjiszy1lo, Ghost, Phantom

Course of action

Patched, configuration, FortiGuard

All those vulnerabilities have been considered by **FortiGuard** and **patched** in latest versions of **FortiOS**.
Last tips in a nutshell:

- Check that your organization FortiGate firewalls are up to date or at least have a minimum version as follow:
  - **6.4.1** or later
  - **6.2.4** or later
  - **6.0.10** or later
- Check that Fortigate firewall's LDAP server, if enabled, has both **secure** and **server-identity-check** options **enabled** to prevent **CVE-2019-5591** exploitation.
- **Network segregation implementation** and **multifactor authentication** are strongly recommended