# 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

May

sogeti
Part of Capgemini

# Weak signals for Strategic CTI

## Ransomwares will cause further damages

https://www.fortinet.com/blog/threat-research/newly-discovered-function-in-darkside-ransomware-variant-targets-disk-partitions/

*Fortinet IR team* observed that a new variant of #Darkside doxware seeks out partitions in a multi-boot environment to create further encryption damage. For this, such variant interrogates the disk drive on an infected system to locate all partitions present (in the same vein as #Petya ransomware), then it mounts additional partitions and **encrypt the files on all available partitions**.

Another outstanding capability of new Darkside variants is to seek out **domain controllers** to connect to its **active directory via LDAP** anonymous authentication, thus enabling reconnaissance capabilities to **encrypt** writable **network shares.** To keep surmise, #Darkside strains **avoid account names** such as **C$** and **ADMIN$** that could **trigger an alert**.

Maybe more threatening is that such ransomware capability actually echoes the one spotted recently by *malwarehunterteam* **being the first of a kind** where for each object found, a customized sample (for the #XingLocker Team sold by the operator of #MountLocker) leveraged Active Directory-related APIs to perform **reconnaissance and spread to other devices**. Enabling the **worm** feature is achieved via the /NETWORK command line upon executing the ransomware. Read the blog of Chuong dong where a **Yara rule** is provided to detect this type of variant.

In the same vein, *ANSSI* reported this year a sample of #RYUK with **worm-like capabilities** (though it self-propagate via the use of scheduled tasks) on which we already alerted and provided tailored detection rules. In previous times #Wannacry leveraged NSA 0-day ETERNALBLUE and DOUBLEPULSAR exploits.

We must underline that **doxware operators** can now afford the market of 0-day vulnerabilities as demonstrated/claimed by #Babuk on **VPN technologies** but also in **Accellion's legacy File Transfer Appliance** *(FTA)* of an unknown cluster in association with #Cl0P **ransomware** as privileged entry points.

Worm, recon, ransomware, Darkside, Mountlocker, XingLocker, RYUK, Petya

**Darkside** ransomware code is optimized and posses the most mature and impactful capabilities
(see threat highlights and spotlights for details)

- A unique capability of **Darkside** is **to mount additional partitions** to further **encrypt them**
- Another peculiar function is to **enumerate and attempt encrypting network shares** with low permission levels

Such **worming/reconnaissance and additional partition encryption capabilities could** encounter a great success **by the top-tier doxware/ransomware operators** in a near future

- **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 known **vaccines shared by CTI** on specific threats
- **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 Highlights

# Threat highlights

## Ransomware-as-a-Service Landscape evolution

https://www.crowdstrike.com/blog/how-ransomware-adversaries-reacted-to-the-darkside-pipeline-attack/

The huge collateral damages that stemmed from the last victim of #Darkside On May 10, 2021 (being responsible for the disruption of the Colonial Pipeline networks) is colliding with heighten diplomatic tensions between the USA and Russia.

The pressure between the two superpowers first cranked up in the wake of the #Solarigate that led to the massive US government cybersecurity breach while the U.S remain a prime target of the top-tier ransom-doxware ecosystem.

More recently, one of the last #Babuk's victim (Washington D.C Metropolitan Police department) also triggered investigations from the FBI forcing its operator to shift TTPs towards Open source RaaS while focusing on the birth of a new leak platform dubbed *"Payload.bin"*.

As a result, RaaS operators such as **RIDDLE SPIDER** (#Avaddon), **PINCHY SPIDER** (#REvil), **Carbon SPIDER** (#Darkside) or #Babuk' operator either attempted to calm tensions respectively by promising to be more cautious in the filtering of their targets with an extended whitelist and/or swearing to be apolitical and not tighten to a nation-state (*i.e.*, Russia).

In the meantime **three major hacking forums banned RaaS** and **broker access advertisements** while the popular cryptocurrency mixing service #Bitmix leveraged for money laundering stopped its operations. #AKO and #Everest DLS disappeared,

However, we anticipate with a **medium high confidence** that the situation only forced those threats to snick out (while not paying their affiliates for Darkside) **to better reappear, soon enough**, with a new brand. This hypothesis is substantiated by the fact that their economical business model was very profitable (of about $90 millions in the past nine months, according to Elliptic for #Darkside).

Worm, recon, ransomware, Darkside, Mountlocker, XingLocker, RYUK, Petya

## Carbon Spider (Darkside)

**Along the year 2013**
Targeting #Hospitality and #Retail sectors via the hack of the cloud-based Oracle MICROS solution

**In 2016**
Part of the group split off to form **Cobalt Spider** and continue to focus on the financial sector

**April 2020**
Shift its operations onto #Big-Game-Hunting (BGH) pinched by Covid-19 crisis and POS shrinkage

**August 2020**
They rent **Pinchy Spider** (REvil RaaS) until **Carbon Spider** operated its own variant based on the code of #Revil

**November 2020**
#Darkside is officially a #RaaS appetized on Russian forums

**March-April 2021**
#Darkside provides a "call service" and DDOS capabilities integrated into the affiliate's management panel to pressure victims

## Colonial Pipeline attack

**6th of May 2021**
**Carbon Spider' affiliates** hit **Colonial Pipeline** that shut down the biggest U.S. gasoline pipeline, #stealing 100 gigabytes of data

**7th of May 2021**
Colonial Pipeline Paid Easter European Hackers nearly **$5 Million in ransom**

**8-9th of May 2021**
FireEye & U.S. Government (#WhiteHouse, the #FBI, CISA and #NSA) assist attack response
**Biden administration** assists Colonial Pipeline attack recovery effort

**10-11th of May 2020**
The #FBI issued a statement confirming that **Carbon Spider is responsible** for the compromise of the Colonial Pipeline Networks.
The #CSIA and #FBI issued a cybersecurity advisory

**13th of May 2020**
The **DLS was 'shutdown'** but **'New infra for other tools' were reported** by CrowdStrike, suggesting that **this threat is still alive**

sogeti
Part of Capgemini

# Cyber-Weather Spotlight

## APT

### Tonto Team (*Karma Panda*)

**Tonto Team** (aka Karma Panda, HartBeat) is a **Chinese state-sponsored APT group** first seen in 2009. Its members likely come from the Shenyang Military Region Technical Reconnaissance Bureau linked by several researchers to the Unit 65017 of the Chinese People's Liberation Army. #Tonto seems to be tasked to target the Chinese near abroad as the majority of its **cyber espionage campaigns** are **oriented against South Korea, Japan or Russia**.
In April 2021, a Chinese APT cluster used the new #PortDoor backdoor to target the Rubin Design Bureau which is a **Russian defense contractor that designs nuclear submarines** for the Russian Navy. Tonto is one of the most probable perpetrator of the attack with the other Chinese group #TA428 according to Cybereason researchers.

Tonto Team, Karma Panda, China, PLA, Russia, Submarines #

China

- Defense
- Government
- Financial
- IT
- Media

- Bisonal malware
- RoyalRoad RTF weaponizer

## E-crime

### Darkside

#Darkside is ransomware that leverages doxing tactics first spotted in August 2020 and believed to be operated by the infamous eCrime group Carbon Spider aka #Carbanak, #GOLD NIAGARA, GOLD WATERFALL, FIN7, ITG14. Darkside follows the #Ransomware-as-a-Service (RAAS) model developing an affiliation program.
On a statement, Darkside published that one can assimilate to an apologize saying that their "goal il to make money, not creating problems for society". Due to the highly disruptive impact of their last attack, the FBI could lead dismantling offensive operation against Darkside that remains inactive.

Darkside, Carbon Spider, Carbanak, RaaS, Colonial Pipeline, FBI #

C.I.S

- Global

- Vmware ESXi targeting
- VoIP calls threatening

## Vulnerability

### Codecov

On **April 1st, 2021**, #Codecov discovered a rogue modification of its bash uploader allowing the upload of sensitive client's information **like tokens and credentials**.

Several companies like IBM and Rapid7 reported that they were only lightly if not impacted, but Codecov is used by hundreds of companies. Such a data leak could allow the attackers to step into their internal networks. **No attribution was made public**.

Codecov, data breach, supply chain attack #

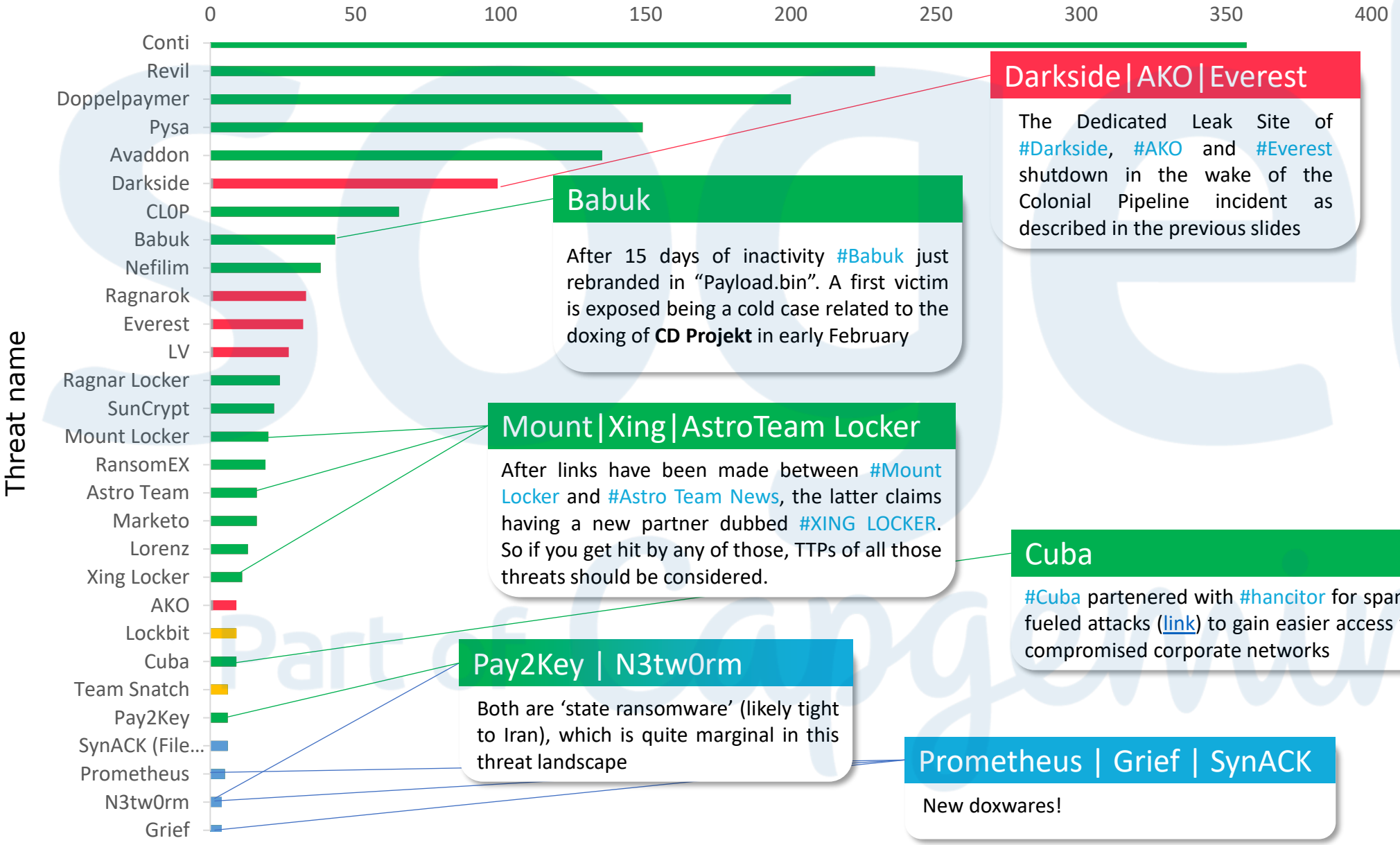
### Course of action

Patched, configuration, #

- Impacted clients received an advisory by Codecov
- Change any Codecov credential or token

# Cyber-Weather

## Evolution of Doxwares




### Darkside|AKO|Everest

The Dedicated Leak Site of #Darkside, #AKO and #Everest shutdown in the wake of the Colonial Pipeline incident as described in the previous slides

### Babuk

After 15 days of inactivity #Babuk just rebranded in "Payload.bin". A first victim is exposed being a cold case related to the doxing of **CD Projekt** in early February

### Mount|Xing|AstroTeam Locker

After links have been made between #Mount Locker and #Astro Team News, the latter claims having a new partner dubbed #XING LOCKER. So if you get hit by any of those, TTPs of all those threats should be considered.

### Cuba

#Cuba partenered with #hancitor for spam-fueled attacks (link) to gain easier access to compromised corporate networks

### Pay2Key | N3tw0rm

Both are 'state ransomware' (likely tight to Iran), which is quite marginal in this threat landscape

### Prometheus | Grief | SynACK

New doxwares!

### Legend

- Shutdown/Ceased
- Online & active
- Online & inactive
- New this month