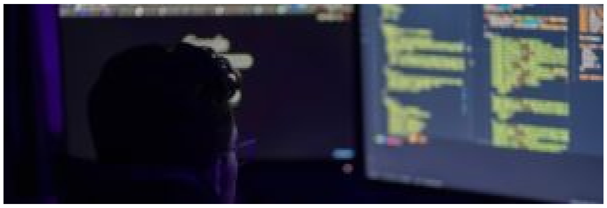
Annual Threat trends 2021

intrinsec.com/annual-threat-trends-2021/

Equipe Cyber Threat Intelligence February 8, 2022



Surge in ransomware attacks

2722

That's **the total number of ransomware attacks claimed in 2021**, corresponding to 7 claims per day

Targeted geography
When looking at the victimology of ransomware operators, one significant fact stands out: the geographical distribution of victims. Although few countries have been spared (108 countries targeted in total), this victimology points to two major trends :
– North America and Western Europe entities represent priority targets for these actors
– The Commonwealth of Independent States (CIS) and Russia remain untouched areas by these attacks

Most active ransomware operators in France
The majority of incident responses involving CERT Intrinsec have been from actors whose attribution cannot be certain. However, several cases have been explicit enough to be able to determine with certainty the nature of the ransomware operators. This year, among the observed cases, the most prolific actors were Conti, Darkside, Ryuk and Lockbit. Our daily monitoring of data leak websites shows that these actors remain in the top 10 most active ransomware affiliates against French entities (see Figure 1.)

Most common techniques used by the most active ransomware operators
We have analyzed the tactics, techniques and procedures employed by the 10 most active ransomware operators in 2021. This analysis reveals that the following techniques are shared by at least 6 of the 10 selected groups :
– Initial Access: External Remote Services (T113)
– Execution: Command and Scripting Interpreter (T1059)
– Defense Evasion: Impair Defense (Disable or Modify Tools) (T1562.001)
– Discovery: File and Directory Discovery (T1083)

Top 10 most active ransomware against France in 2021

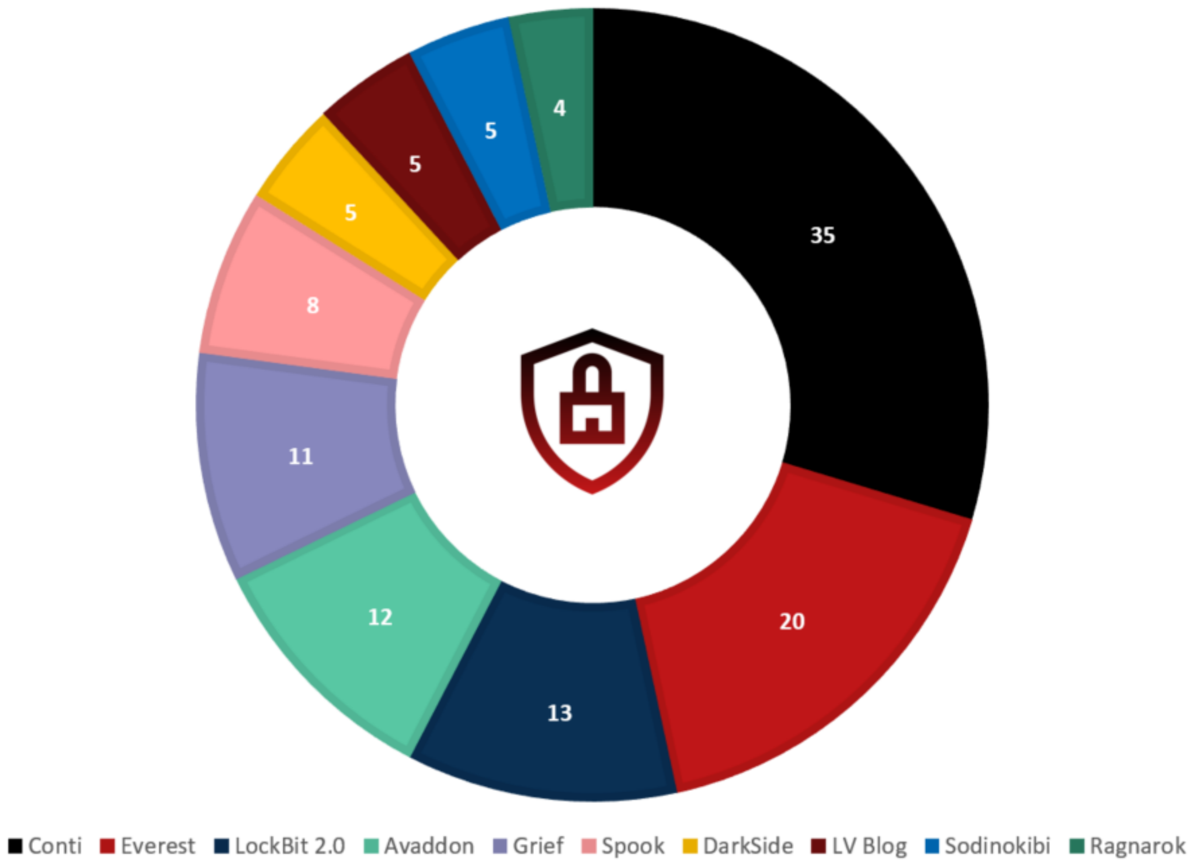


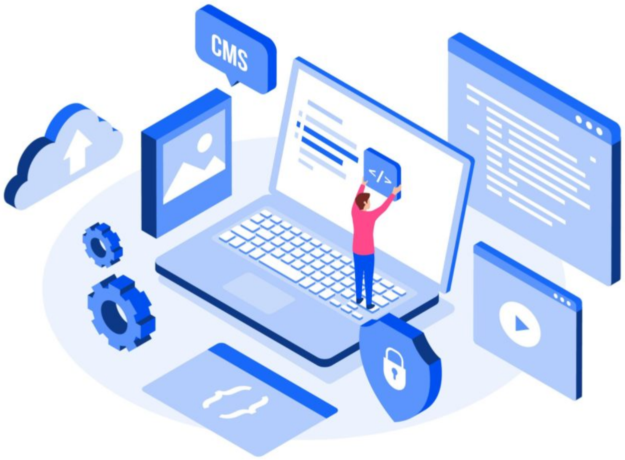
Figure 1. Most active ransomware operators against French entities, based on data leak website monitoring

Initial access vector: vulnerabilities and phishing on the top

Our SOC and CERT operations as well as our monitoring on hacking platforms shows that phishing and vulnerabilities exploitation remain the most common techniques employed by threat actors to gain an initial foothold on targeted networks.

Exploitation of remote access appliances

This is a trend largely documented in 2020 after the beginning of the Covid-19 pandemic, RDP and VPN appliances used by employees to access their network remotely increased the attack surface of the corporate network. On the 49 missions covered by our CERT throughout 2021 and with a pandemic still ongoing, Citrix, Fortinet, SonicWall and Pulse appliances have been largely exploited by threat actors to compromise networks. The interest in RDP is also largely observed on hacking platforms with a lot of initial access brokers specialized in selling this type of product as shown in the next slide.



Most frequent vulnerabilities

Among the most exploited vulnerabilities identified by our CERT in 2021, Microsoft Exchange Server and ProxyShell exploits in particular are far ahead in terms of frequency with 18% of incidents involving one of these vulnerabilities. However, more than 20% of all the vulnerabilities observed by our CERT as being actively exploited in 2021 are dating back from 2020, 2019 and 2018. Patches are not always applied immediately, allowing threat actors to exploit vulnerabilities months after their public releases. For example, ZeroLogon's vulnerability CVE-2020-1472, discovered in 2020, has continued to be exploited by actors such as Conti and Darkside during the first half of 2021. This interest for vulnerabilities demonstrated by threat actors is largely supported by our SOC operations as in 15 496 detections in 2021 "Execution of malicious code attempts" remains one of the most observed one (13%).

Phishing

Two key statistics highlighted by our SOC and CERT reveal that threat actors keep using phishing to get an initial foothold on a network :
– 12% of the incident responses conducted by CERT Intrinsec involved phishing attempts;
– The incident type "malicious link" is among the most observed one by our SOC (alongside

aggressive port scans, aggressive subnet scans and bruteforce attempts)
This initial access technique is used by threat actors distributing loaders such as Emotet, IceID, Bazar Loader or QakBot. This type of threat continues to target corporates and is often combined with other threats such as the exploitation of known vulnerabilities or ransomware, making them potentially

Cybercrime marketplace still going strong

The activity on cybercrime marketplaces keeps growing, as well as shifting from Dark towards Surface Web platforms. Our investigations conducted on these networks throughout 2021 identify particularly strong demand for the diverse typologies of criminal goods and services as follows :

33% Vulnerabilities

Pronounced interest in buying/selling Remote Desktop Protocol configurations for fraudulent access to systems of companies operating across multiple sectors. SQL injections to target vulnerable websites are also in high demand.

33% Customer Data

Stolen customer databases, containing sensitive information such as connection credentials to diverse online services or financial data, remain one of the most popular goods on cybercrime networks.

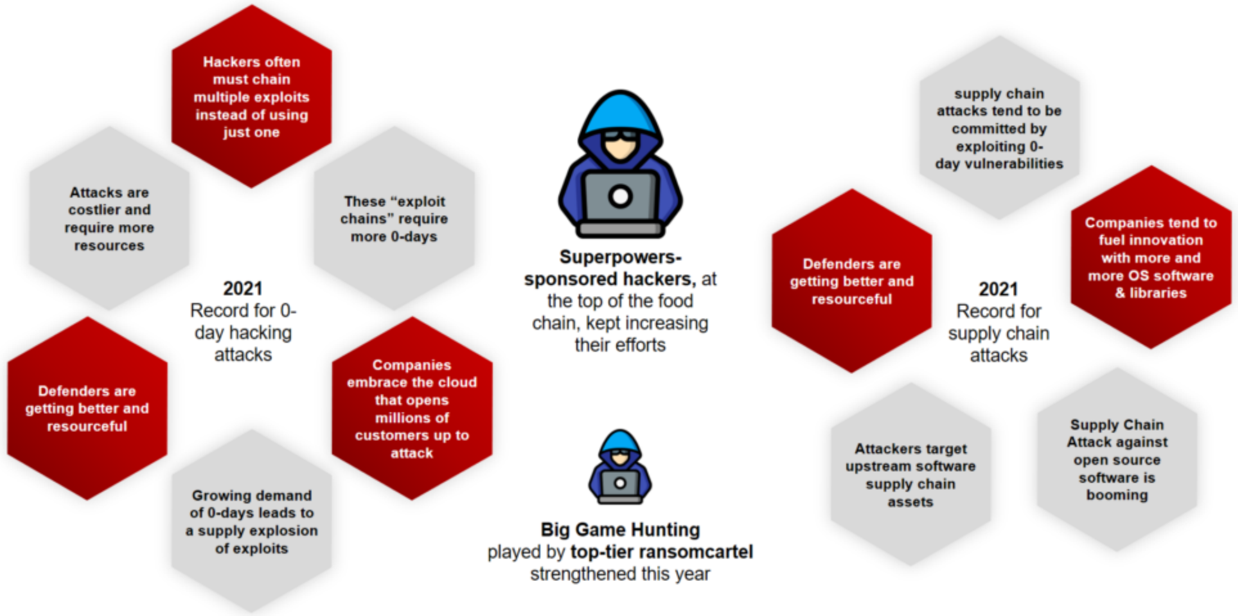
29% Company Data

Employee connection credentials to internal companies' internal services, i.e. efficient vectors of compromise, are a sought-after product. Likewise for internal sensitive or confidential data, such as strategic projects or HR information.

5% Counterfeit goods / services

Demand for counterfeit goods and services on criminal marketplaces is persistent, although handled to a lesser extent from the viewpoint of CTI teams (dealing mostly with cases of fraudulent configurations imitating real services).

Zero-days and supply chain attacks


Hackers often must chain multiple exploits instead of using just one
Attacks are costlier and require more resources
These "exploit chains" require more 0-days
2021
Record for 0-day hacking attacks
Defenders are getting better and resourceful
Companies embrace the cloud that opens millions of customers up to attack
Growing demand of 0-days leads to a supply explosion of exploits
Superpowers-sponsored hackers, at the top of the food chain, kept increasing their efforts
Big Game Hunting played by top-tier ransomcartel strengthened this year
supply chain attacks tend to be committed by exploiting 0-day vulnerabilities
Defenders are getting better and resourceful
2021
Record for supply chain attacks
Companies tend to fuel innovation with more and more OS software & libraries
Attackers target upstream software supply chain assets
Supply Chain Attack against open source software is booming

Most impactful 2021 flaws involving Zero-Day vulnerabilities and/or a supply chain attack

JANUARY 2021

Solar winds

05/01/2021

US intelligence agencies formally accuse Russia of association with the SolarWinds attack that dates back in September 2019

Russian-state sponsored attackers inserted a backdoor into SolarWinds Orion IT monitoring software updates to 18,000 government entities and Fortune 500 companies. Through this, malware was distributed to at least nine US federal agencies and more than 100 companies

MARCH 2021

Accellion FTA

01/03/2021

Accellion releases a last patch based on IR mandiant report fixing a series of 0-day vulnerabilities affecting Accellion File Transfer Appliance compromise that started back in

December 2020;

Attacks carried out by a Russian-speaking cybercriminal group known as FIN11 using zero-days against Accellion FTA servers hit around 100 companies across the world in December 2020 and January 2021. In some cases FIN11 leveraged CLOP double extortion infrastructure

Microsoft Exchange

03/03/2021
Mass exploitation of Microsoft on-prem Exchange RCE dubbed Proxylogon. Indications of retroactive exploitation dating back two weeks

In March 2021 Chinese cyber espionage groups exploited four vulnerabilities in Microsoft’s on-premises Exchange Server software. This compromised more than 100,000 servers worldwide.
Beyond the intelligence gathering from emails, the latter were abused for hijack existing email threads by the infamous Emotet botnet

JULY 2021

Kaseya

02/06/2021
Pre-auth remote code execution of 0-day exploits against Kaseya VSA server

At the end of June Kaseya, which provides a service to manage enterprise IT infrastructures, was compromised by the Russia-based REvil criminal gang. Kaseya can deploy software updates (patches) to the systems under management, so REvil used this to push ransomware to all Kaseya customers, affecting thousands of companies worldwide. 100 had some measure of impact from the attack, with another 25 of those experiencing significant data loss.

DECEMBER 2021

Log4J

01/12/2021
The first proof of exploitation attempts would have been observed by Cloudflare and Cisco Talos

This open-source component is widely used across many suppliers’ software and services. Not only numerous state-sponsored threats crystallized on the situation as well as top-tier ransomcartels but also coin miners and botnets.