

Ransomware Targeting Italy- May 2022

Soufyane Sassi

Senior SE / Recorded Future

Outlook

Ransomware as a Service

- Law Enforcement Actions - removal of more players like REvil and Blackmatter
- Expect more RAAS groups to emerge to fill vacuum (e.g. ALPHV)
- Expect Lower barrier to enter RAAS market which will lead to more irrational activity, unexpected impacts and risks

Actions

- Monitor TTP's of RAAS groups and share with teams to identify possible gaps in process & controls to minimise impact
- Takedown malicious infrastructure
- Threat hunt for hand on keyboard activities unique to Ransomware and precursors (IPs/domains/tools)
- Search dark web for Initial Access Brokers targeting Australia
- Search dark web for employee credentials (Microsoft: 70% attacks from credential recycling)

Ransomware Summary 2021

28/34

Ransomware Groups had Law Enforcement Action Taken against or “retired” in 2021

131_(UK) / 2865

Total Victims posted in 2021
(109 Finance / 396 2022 YTD / 51 UK / 0 Finance)

\$590 Million

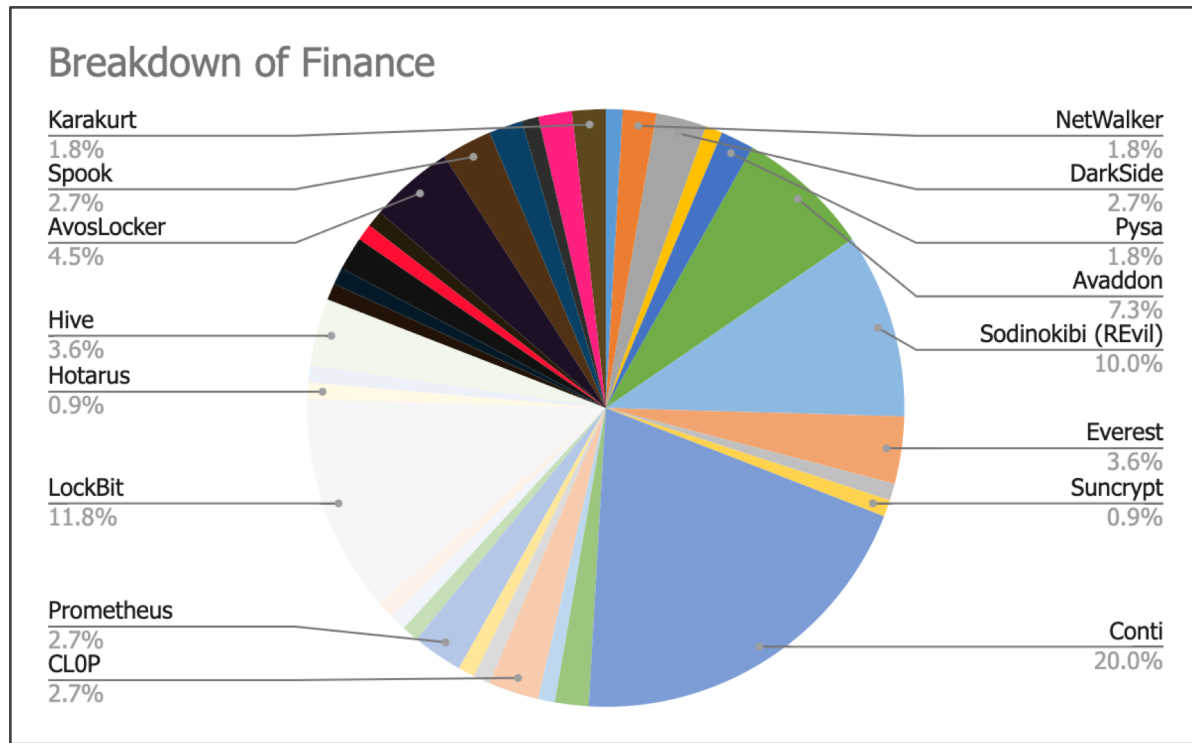
The amount of ransom payments made in the first half of 2021 according to FinCEN

100% increase

Data breaches inc Ransomware from 2020 to 2021 ([VDBR report 2021](#))

Industry Targets - Finance breakdown

- In 2021, Recorded Future analysts believe that ransomware operators and their affiliates are opportunistic by nature and do not typically focus on specific industries or geographic regions
- Select and pursue organizations based on accessibility, opportunity, and factors such as the ability to pay large ransom amounts read ***significant company revenue***
- Finance - ***109 / 4267***
observed published victims



Ransomware Extortion

- RaaS has driven extortion to become significant part of attack
- If RAAS affiliate cannot extort ransom payment they look for other ways to blackmail victims
- Reputational risk/harm impacted
 - Loss of service
 - Personal Identifiable Info
 - Executive emails
 - Mergers & Acquisition
 - Denial of Service



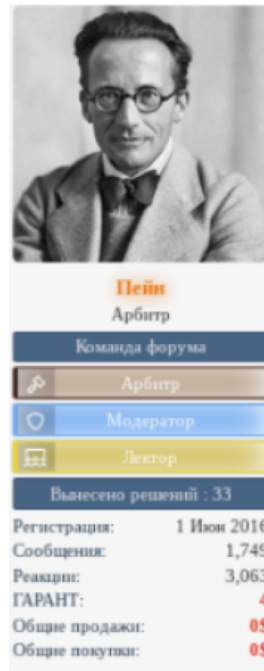
Source: Reddit

Fraud

Fraud Guides:


- Fraud Tutorials and courses are available on the Dark Web and underground communities, providing 'how-to' guides on committing Fraud.
- **GOLDIE ENROLL 5.0** course is specifically tailored to enable cyber criminals to commit online banking fraud.
- Messaging Platforms (Telegram), Dark Web Forums and Paste Sites (Pastebin) are common channels for Threat Actors to advertise compromised bank accounts.
 - There are specific terms taught in the Carding Community to be aware of e.g. *'Fullz, Zaliv, Karton'*


The Business of Fraud: Fraud Tutorials & Courses




"Your task is to mimic a real user. Every little detail counts: get a proxy, as close to the cardholder's ZIP code as possible, start from a search engine, browse to an online store, warm it up by spending time to check various related products. If you are about to card a laptop, pretend to be a grandma looking for a present for her grandson. Don't act as a carder and you won't look like one."

GOLDIE ENROLL
C R E D I T U P D A T E

 TIB BANK
AVAILABLE CREDIT:7.700\$
BEAUMONT|TX|77726
инст миники | nonvbv
price:90\$


 FIRST COMMUNITY BANK
AVAILABLE CREDIT:880\$
WV | Craigsville | 26205
инст миники
change billing | change number
price:50\$


 PNC BANK
AVAILABLE CREDIT:24.000\$
OH | Cleveland | 44125
инст миники | nonvbv | ssn+dob
price:90


◆ CENTRAL BANK
AVAILABLE CREDIT:4.800\$
SANTAQUIN|UT|84655
инст миники
price:200\$

◆ VIRGINIA F.C.U.
AVAILABLE CREDIT:16.000\$
GOODE|VA|24556
инст миники | noconf mail
price:260\$

◆ NORTHWEST SAVING BANK
AVAILABLE CREDIT:2.600\$
NY|14120
инст миники
price:170\$

 PNC BANK
AVAILABLE CREDIT:4.700\$
FREDERICKSBURG|VA|22407
инст миники | nonvbv | ssn+dob
price:65\$

 PNC BANK
AVAILABLE CREDIT:25.000\$
FORT LAUDERDALE|FL|33308
инст миники | nonvbv | ssn+dob
price:100\$

 PNC BANK
AVAILABLE CREDIT:40.000\$
IN | city:Brownstown | zip:47220
инст миники | nonvbv | ssn+dob
price:150\$

 ALLIANT C.U
AVAILABLE CREDIT:14.700\$
FAIRFIELD|OH|45014
инст миники
price:130\$


Fraud

Tactics, Techniques and Procedures (TTPs)

- Threat actors use a diverse set of sophisticated TTPs - Identity Theft, Corporate Network Compromise, Ransomware, Money Laundering and Social Engineering Attacks
- Services are primarily advertised on top tier Russian forums such as **Exploit, XSS** and **Verified**
- An attacker would be able to purchase things like account credentials, session cookies and browser fingerprints and use these in combination with PII.
- Bots sold on **Genesis Store** can provide a wealth of financial information.

The Business of Fraud: Tax Refund Fraud

bl33d
Mindcoms
●●●●



Paid registration
● 11
144 posts
Joined
11/15/19 (ID: 97214)
Activity
cnam / spam
Deposit
0.033000 B

Posted January 4

Report post

Each folder represents each client , in each folder you will find W2 scans + DL scans , sometimes there is ssn card scans but occasionally you may find W2 and dl Scans of multiple persons in one folder. In some you will find W2 history of a client from 2017 -2019 DL scans have good quality and 70++ % have good expiry dates .

<http://prntscr.com/wgbfb2> DL scans front
<http://prntscr.com/wgbgxx> DL scans back
<https://prnt.sc/wgbjxx> W2 Scans
<https://prnt.sc/wgbmmv> MULTIPLE SSN SCANS
<https://prnt.sc/wgbonr> MULTIPLE DL SCANS
<https://prnt.sc/wgbr3u> DL + SSN SCAN FRONT
<https://prnt.sc/wgbrx9> DL + SSN SCAN BACK
<http://prntscr.com/wgbthz> W2

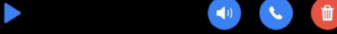
Start : \$11,000
Step : \$250
Blitz : \$15,000

+

Quote

+1 (201) 584-0553
Hackensack, NJ
October 4, 2021 at 11:33 AM

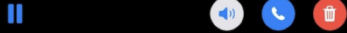
0:00 -0:50



Transcription
"Hello this is Mary Fletcher state number agent FF694 and this is a notification call for department of financial relief services and the purpose of this call is to inform all US citizens on state list that have tax that about the new zero tax oh tax debt relief program that was recently put into affect by the Biden ministration and is open for enrollment the new zero tax owed relief program will allow you to significantly reduce or eliminate altogether your tax debt as it is now considered temporary Lee non-collectible however you might be left to enroll into the program as it is only open for a very limited time so to enroll in the zero tax oh tax debt forgiveness program please call me back at my FaceTime number..."

+1 (208) 470-5071
Rathdrum, ID
November 12, 2021 at 5:18 PM

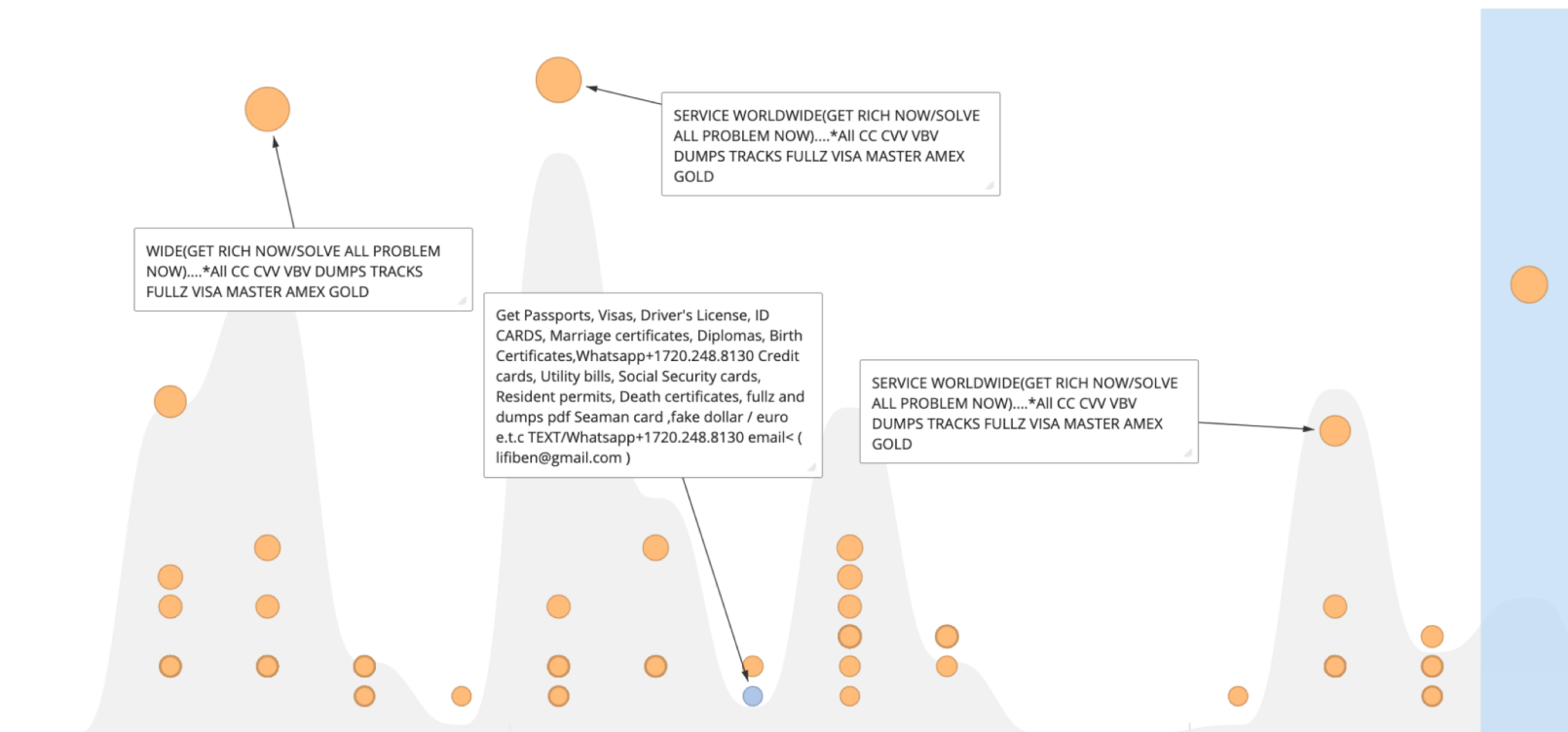
0:08 -0:57



Transcription
"My name is Martha Thompson state number SS 681 this is a notification from our Department of tax debt and financial settlement services at tax experts the purpose of this call is to inform all US citizens on our state list about the new tax debt compromise program this program is now open for enrollment the new tax owed compromise program will allow you to significantly reduce or illuminate your tax debt your tax debt can possibly now be considered Temporarity non-collectible however you must elect to enroll in a program now it is only open for a limited time to enroll in the tax debt comoromise program please call me back at mv

Paste Site, "fullz"

Click To Add Annotation

View Query: <https://app.recordedfuture.com/live/sc/3vCuEsWLEVoC>

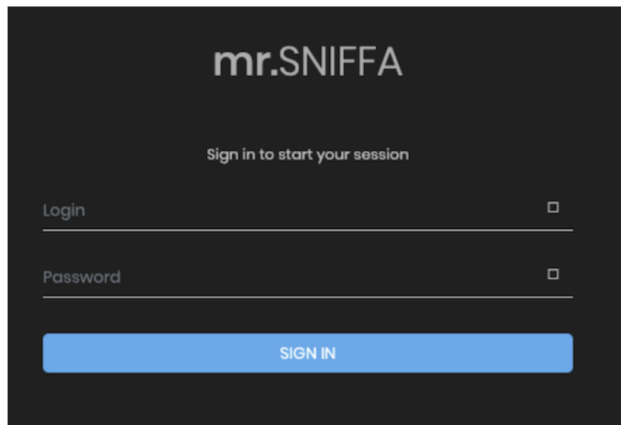
Skimmers / Sniffers

- Dark web threat actors are using high-tier dark web sources to advertise and sell customised JS Sniffers that are defined and regularly updated to harvest credentials once injected into a website's payment process. I.e MageCart.
- Customised sniffer variants contain multiple capabilities and functionalities.
- Threat Actors such as "Sochi" (Inter Sniffer creator) and "Billar" (Creator of JS Credit Card Sniffer Mr Sniffa), provide access to Sniffers on well-known underground communities such as Exploit forum for varying costs.

[Credit Card 'Sniffers' Pose Persistent Threat to Growing E-Commerce Industry](#)

Some advertised features:

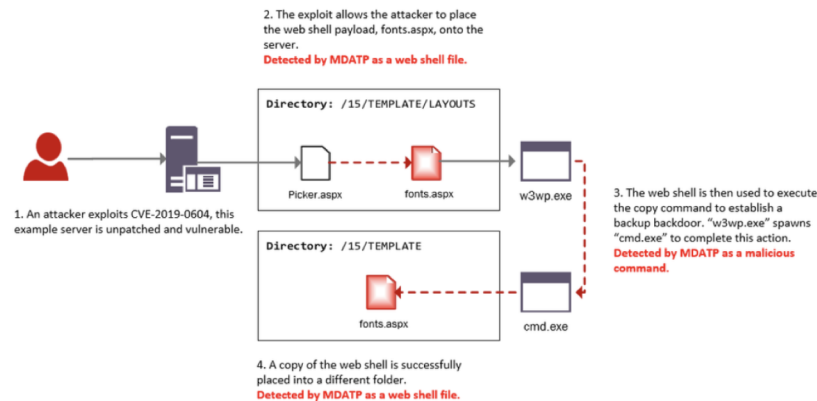
- Regular Updates
- Checked all compromised BIN
- Organised stolen payment cards in a single format
- Deleted repeating payment cards
- Grabbed login / password and billing/shipping addresses from cards



Webshells & Skimmers

- Cybercriminals are increasingly using web shells to establish command and control over retailers' servers during payment card skimming attacks.
- This puts eSkimming / Sniffers at the top of the threats to the ecosystem.
- Deploying Webshells allows Fraudsters to maintain access to compromised servers, where they can deploy additional malicious files, facilitate lateral movement and remotely execute commands.

[Visa Describes New Skimming Attack Tactics](#)



Common Webshell Installation: Microsoft.

BANK INFO SECURITY

Topics ▾ News ▾ Training ▾ Resources ▾ Events ▾ Jobs ▾

TRENDING: Live Discussion: 4/5 | Is Your Secure Email Gateway Really Necessary? Blocking the Attacks Your SEG Nev

Account Takeover Fraud , Card Not Present Fraud , Cybercrime

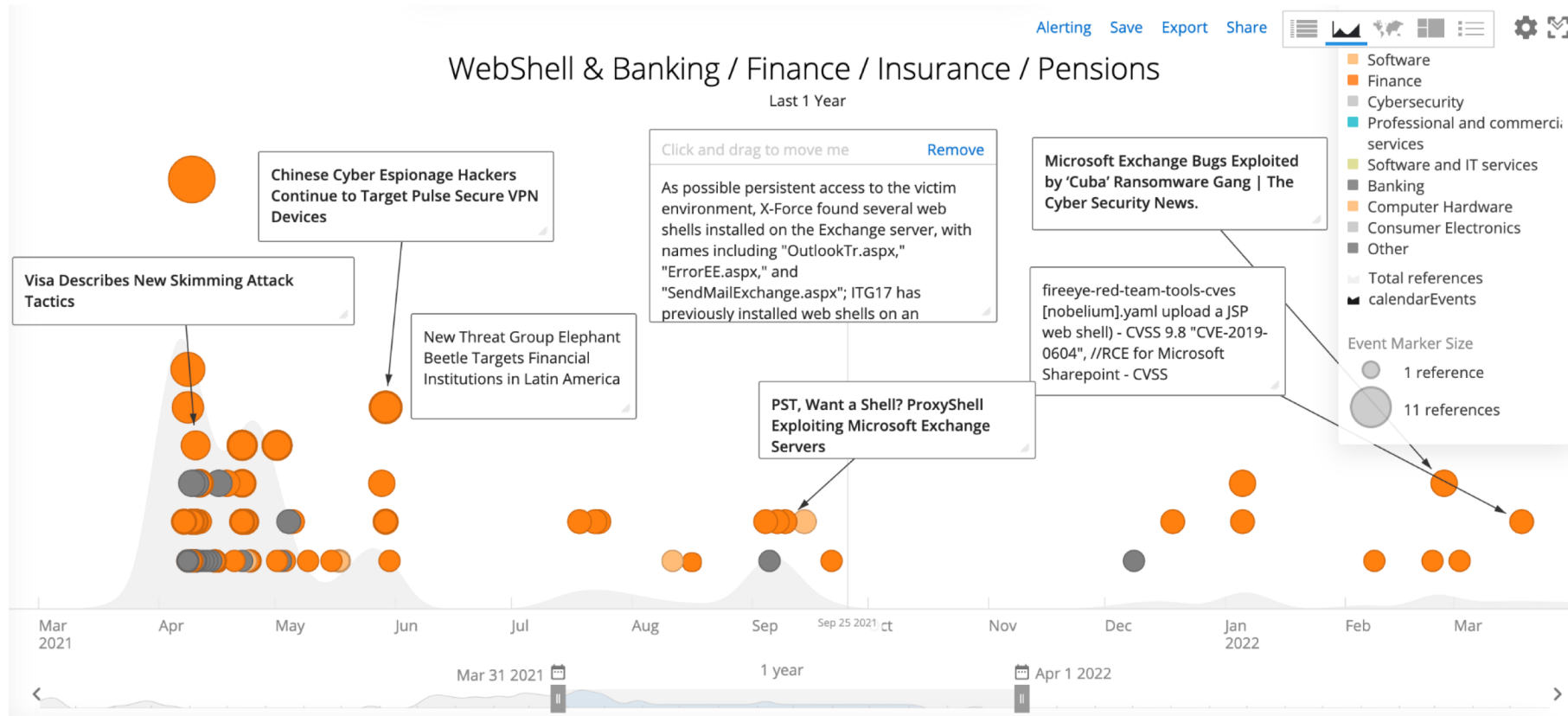
Visa Describes New Skimming Attack Tactics

Cybercriminals Using Web Shells to Control Retailers' Servers

Doug Olenick (👉DougOlenick) · April 9, 2021



Get Permission



View Query: <https://app.recordedfuture.com/live/sc/1n3F7mwu6jD5>

Outlook



- **Cyber Insurance:** more complexity and rising costs likely to make less appealing to organisations in light of Merck legal ruling
- **Cyber Policy:** new, more powerful US cyber laws could be less likely to pass through Congress as Biden and Democrats lose out in mid-term elections in late 2022
- **RAAS:**
 - Increase of US, UK & EU governments focus on crypto payment restrictions to combat
 - Russia / Westen tension lead to less Russian action to stop actors inside Russia
 - RAAS groups improve operational security to minimise LEA disruption
- **Log4Shell:** monitor Log4S vuln for latest TTP's utilising it (e.g. IP's, ransomware, crypto-mining etc)
- **Deepfake:** Expect malicious actors to shift for blackmail, Identity theft and social engineering uses. Read our [Deepfake Report](#)

Ransomware - Top 5 Groups targeting Financial Services

- **Lockbit 2.0** - encrypt 100GB of data in < 5 minutes (as advertised). Recruitment of insiders.
- **Conti** - ties to Ryuk. Most aggressive group of 2021. Avg payment <\$100k USD. Multi-threaded - faster encryption achieved.
- **BlackMatter** - since July 2021. “Best features of DarkSide, REvil, and LockBit”. Has both Windows & Linux variants for ESXi and NAS support.
- **Hive** - since June 2021, targets Windows, Linux, and ESXi devices. Operators have shown a particular interest in healthcare organizations, although finance and banking also targetted.
- **Clop** - AKA FANCYCAT. Tool affiliated with many threat groups that appear Russia based inc FIN11, TA505, UNC2546, UNC2582, and Hive0065. Used in arsenal of tools in org attacks.