eSENTIRE

Unmasking VENOM SPIDER

The Hacker Behind the Cyber Weapon of Choice for Two of Russia's Most Notorious Internet Crime Gangs

by Joe Stewart and Keegan Keplinger,
Security Researchers with eSentire's Threat Response Unit (TRU)

Executive Summary

For the past 16 months, eSentire's security research team, the Threat Response Unit (TRU), has been tracking one of the most capable and stealthy malware suites—Golden Chickens. Golden Chickens is the "cyber weapon of choice" for three of the top money making, longest-running Internet crime groups: Russia-based FIN6 and Cobalt Group and Belarus-based Evilnum. The three criminal operations are estimated to have collectively caused financial losses over USD $1.5 billion. This report unveils the identity of the threat actor behind Golden Chickens—who goes by badbullzvenom—and outlines how he was found.

Key Findings

Who is badbullzvenom? Reading through the history of the threat actor's posts on the Russian-language hacker forum, Exploit.in, TRU found multiple mentions of the badbullzvenom account being shared between two people. From the posts, we learn the following about badbullzvenom:

- They claim to be from Moldova
- They speak Romanian, French and English
- They claim to work with Russia-based Cobalt Gang (this is also evident in public analysis of Golden Chickens campaign IOCs)

Who is "Frapstar" and What is His Connection to badbullzvenom?

Numerous other data points in the report connect a second threat actor, who goes by "Frapstar" and the username badbullzvenom. He self-identifies as "Chuck from Montreal" – an alias. In addition to speaking French and having a keen interest in buying stolen Canadian credit card accounts, he says he owns a BMW 5 Series automobile, which provides TRU with further leads into the identity of "Chuck".

Conclusion

TRU has discovered "Chuck's" real name, pictures of him, his home address, the names of his parents, siblings, and friends; his social media accounts, his hobbies, and that he owns a small business, which he runs out of his home.

"Chuck", who uses multiple aliases for his underground forum, social media, and Jabber accounts, and the threat actor claiming to be from Moldova, have gone to great lengths to disguise themselves. They have also taken great pains to obfuscate the Golden Chickens malware, trying to make it undetectable by most AV companies, and limiting customers to using Golden Chickens for ONLY targeted attacks. Because of eSentire's investigation, "Chuck" has lost his anonymity. TRU also continues to track improvements in the Golden Chickens source code and discover new Golden Chickens attack campaigns, as recent as July, which tells us at least one threat actor is still actively developing the product and selling it to other cybercriminals. We expect to see further targeted attacks, leveraging this malware, being launched against financial institutions and other organizations in the foreseeable future.

Introduction

eSentire is a leading global provider of Managed Detection and Response security services. For the past 16 months, our security research team, the **Threat Response Unit (TRU)**, has been tracking, analyzing, and defending our customers from one of the most capable and stealthy malware suites on the Cyber Underground – Golden Chickens. Golden Chickens is the "cyber weapon of choice" for three of the top money making and longest-running Internet crime groups: Russia-based FIN6 and Cobalt Group and Belarus-based Evilnum. The three cybercrime operations are estimated to have collectively caused financial losses over USD $1.5 billion.

Since 2018, the Golden Chickens suite has been distributed as a Malware-as-a-Service (MaaS). Between April 2021 and April 2022, TRU discovered two significant hacking campaigns utilizing Golden Chickens. During the April 2021 incidents, TRU found corporate employees on **LinkedIn** being targeted by threat actors using fake job offers. One year later the April 2022 campaign uncovered by TRU demonstrated that the attack tactics were reversed, and **corporate hiring managers** were sent fake resumes, of job applicants, laden with malware.

TRU continues to track the Golden Chickens malware, and not only have we detected a new threat campaign that appears to be targeting e-Commerce organizations, we have also discovered the identity of the threat actor/operator behind Golden Chickens. He is referred to by CrowdStrike researchers as **VENOM SPIDER**, and he has been connected to the threat actor "badbullzvenom".

TRU has tracked many of badbullzvenom's Internet activities, going back as far as 2013. We have also discovered badbullzvenom's birthdate, home address, his parents and siblings' names, friends' names, his hobbies, his social media accounts, and one of his side businesses.

It is rare to uncover this level of detail about a threat operator, and it illustrates the breadth and expertise of TRU. This intelligence, including many of the Underground Forum conversations badbullzvenom has had with other threat actors, has been extremely valuable. It has helped us better decipher his Tactics, Techniques and Procedures (TTPs), as well as the origins of the Golden Chickens MaaS and its ongoing operations. With this knowledge, we continue to hone our defenses, protecting eSentire's global customer base from well-orchestrated attacks utilizing the Golden Chickens MaaS.

It is our objective with this report to share our research with other organizations and their security teams so that they might better defend their critical data and applications from threat actors mounting attack campaigns using the Golden Chickens malware suite. The balance of this report includes:

- A brief overview of the FIN6, Cobalt Group and Evilnum cybercrime organizations
- A detailed account of the investigation and subsequent identification of the Golden Chickens MaaS operator
- An analysis of the Golden Chickens malware and the current attack campaign
- Insights and security recommendations from TRU

Golden Chickens' Connection to the Billion Dollar Hackers' Club—FIN6, Cobalt Group and Evilnum

For those not familiar with FIN6, Cobalt Group and Evilnum, they are hands down three of the longest-running and successful financial crime gangs, and it is reported that cumulatively they have caused over USD $1.5 billion in losses.

FIN6

This Russia-based, financial cybercrime group is known as one of the most notorious hacking gangs in the world of cybercrime. They dominated **news headlines** in 2018 when they were cited as being the cyber gang who broke into the online payment systems of British Airways, Ticketmaster UK and top electronic retailer, Newegg, stealing credit and debit card data from millions of customers, as well as stealing Personal Identifiable Information (PII) from British Airways' customers and staff. **British Airways** concluded that during their cyber heist, the hackers siphoned off credit and debit card data (also referred to as card-skimming),and personal data from 425,000 of their customers and staff. As a result, British Airways was slapped with a £20 million (USD $26 million) fine from the Information Commissioner's Office (ICO), a UK government watchdog group. The ICO determined that British Airways did not take the right precautions in protecting the sensitive data of its customers. However, the ICO fine was not the end of the damage caused by the FIN6 breach of British Airways. On July 5, 2021, British Airways settled a legal claim made by a group of the airline's customers and staff, whose data had been leaked during the breach. The settlement was kept confidential, and the airline agreed to pay compensation for qualifying claimants but did not admit liability, according to news sources.

The number of customers affected by the **Ticketmaster UK breach**, at the hands of FIN6, numbered in the millions. In fact, security experts estimate that the 2018 attack impacted 9.4 million customers. The UK ICO determined that the breach led directly to widespread fraud. As such, they levied a fine of £1.25 million on the ticket agency stating that the corporation "failed to put appropriate security measures in place to prevent a cyberattack on a chat-bot installed on its online payment page" – and this violated the E.U.'s General Data Protection Regulations (GDPR).

While top online electronics retailer **Newegg** couldn't specify just how many of their customers' credit and debit cards were stolen, security reports found that the threat actors were inside Newegg's IT network for a month before being detected, giving the cyberattackers a full 30 days to skim many of Newegg's customers. Newegg is estimated to receive over 50 million visitors a month, according to Similarweb, a firm which collects information on site visits.

Conservatively, security firm FireEye estimates that between 2016 and 2019, FIN6 is believed to have stolen 20 million payment cards worth $400 million. The FIN6 gang first gained notoriety in 2014 for their attacks against point-of-sale (POS) machines in retail outlets and hospitality companies but as proven by their attacks against British Airways, Ticketmaster UK and Newegg in 2018, they wholeheartedly moved on to target online payment systems of large e-Commerce companies.

FIN6 Attacks E-Commerce Companies' Payment Platforms with Golden Chickens in Late 2018 & Retail, Entertainment and Pharma Companies' Payment Portals Attacked by Golden Chickens in Early 2019.
Interestingly, intelligence analysts with **Visa** reported that at the end of 2018, FIN6 was specifically targeting numerous e-Commerce companies' payment servers and using malicious documents to infect their targets with the **more_eggs** component of the Golden Chickens malware, as the initial phase of their attack.

That activity mirrors another threat campaign that was reported separately in February 2019 by **ProofPoint researchers**. In these incidents, threat actors were observed attacking retail, entertainment and pharmaceutical companies' **online payments systems** and using malicious documents, laden with the **more_eggs** component of Golden Chickens, to target the companies' employees. The threat actors sent fake job offers to the employees, cleverly using the job title listed on their LinkedIn profiles in their communications. Could FIN6 be behind this Golden Chickens attack campaign?

Later in August 2019, the FIN6 operators launched another malicious campaign, and researchers believe FIN6 was actively going after multinational organizations. Like the February 2019 campaign, employees were spear phished with fake job offers. According to researchers, the threat actors began by targeting handpicked employees using LinkedIn messaging and email.

Between the end of 2018 and April 2021, there have been three distinct **Golden Chickens/more_eggs LinkedIn campaigns** using the same modus operandi (MO). Each campaign targeted corporate employees, utilized their LinkedIn profile, and then social engineered them with bogus job offers, which lead to the **more_eggs component** of **Golden Chickens**.

Cobalt Group

Another Russia-based organized cybercrime gang that has been plaguing financial institutions since at least 2016 and is known to use the **Golden Chickens malware** suite. **The Cobalt Group** is reported to have caused the financial industry over a **billion dollars** in cumulative losses. Their crime spree includes the targeting of 100 financial institutions in more than 40 countries worldwide, allowing the criminals to steal more than USD $11 million per heist.

The Cobalt Group's typical MO was to infiltrate banking institutions by sending spear phishing emails with malicious attachments to bank employees. The Cobalt Group repeatedly used **Golden Chickens** and its **more_eggs backdoor** in their attacks. Once downloaded, the cybercriminals gained access to the infected computer and were able to access the internal banking network. The Cobalt Group was said to have spent months inside the infected networks studying the bank's operations and workflows, including the Society for Worldwide Interbank Financial Telecommunications (SWIFT) bank system.

The Cobalt Group also gained notoriety for its "jackpotting" schemes where they would break into bank servers that controlled the ATMs and manipulate the ATMs to remotely dispense cash at a certain time, in predetermined locations, where money mules waited to collect the cash.

Evilnum

The Evilnum group, believed to be out of Belarus, is best known for compromising financial technology companies and companies that provide stock trading platforms and tools. They target financial information about the FINTECH companies and their customers, seeking out spreadsheets, customer lists, investments, trading operations and credentials for trading software platforms. The Evilnum group is also known to spear phish employees of the companies they are targeting and enclose malicious zip files. If executed, the employees often get hit with the more_eggs backdoor, along with other malware.

Unmasking badbullzvenom—The Threat Actor Behind Golden Chickens

Quo Intelligence first connected VENOM SPIDER to the threat actor "**badbullzvenom**". This attribution was made possible due to a dispute on the Exploit.in hacker forum. In the thread, private conversations are revealed between a Golden Chickens MaaS customer, BlackAngus, and the MaaS provider badbullzvenom. The dispute centered around a sample of the malware appearing in VirusTotal, causing the customer to be banned from the service. Because the actual sample in VirusTotal was linked in the thread, researchers were able to confirm the connection to the Golden Chickens MaaS and identify badbullzvenom as the MaaS operator.

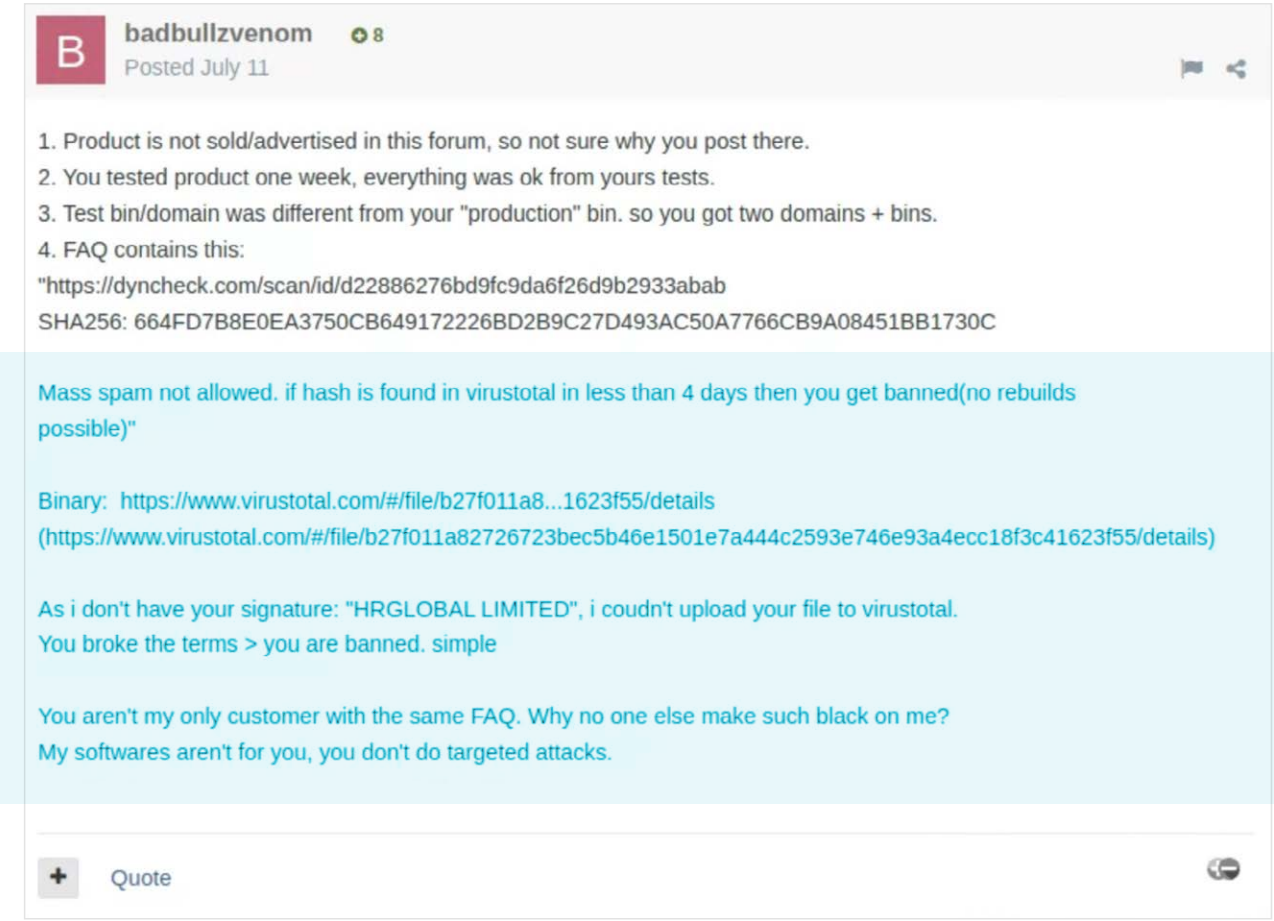

Figure 1—Exploit.in reply to dispute thread. badbullzvenom drops BlackAngus as a customer for breaking his rules and shuts down his access

From the entire content of his posts on Exploit.in, we learn the following information about badbullzvenom:

- They claim to be from Moldova
- They speak Romanian, French and English
- They claim to work with Cobalt Gang (this is also evident in public analysis of Golden Chickens campaign IOCs)

The Connection Between badbullzvenom and "Frapstar"

Digging deeper into Open Source Intelligence (OSINT), TRU studied numerous security reports in order to connect the various forum accounts engaged with the Golden Chickens MaaS, and we found one published by Trend Micro in 2015 titled: *Attack of the Solo Cybercriminals – Frapstar in Canada*, where the threat actor is identified as a lone carder (a criminal who monetizes stolen credit cards) with accounts and multiple aliases (including badbullzvenom) on several hacker forums.

であることを説明できます。サイバー攻撃集団の場合、サイバー犯罪者たちは、地理的に近接した状態で活動を遂行するからです。

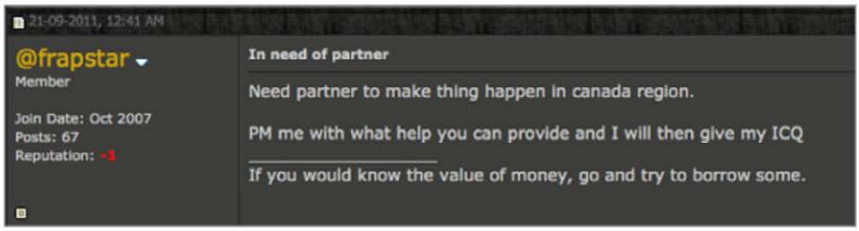

図1：Frapstar が投稿したサイバー犯罪者への「求人募集」

弊社では、この人物に関連するメールアドレスやハンドル名を手がかりにして、他のオンラインフォーラムでの彼の活動も突き止めました。別のフォーラムでの彼の投稿を確認すると、高級車の愛好家で BMW の旧モデル 540i を所有していることも分かります。この BMW関連フォーラム上からは、彼が「Chuck」とも名乗り、モントリオール在住であることも分かります。しかも、投稿でのやり取りのため、ご丁寧に自身の Gmailアドレスまで忘れずに掲載しています。

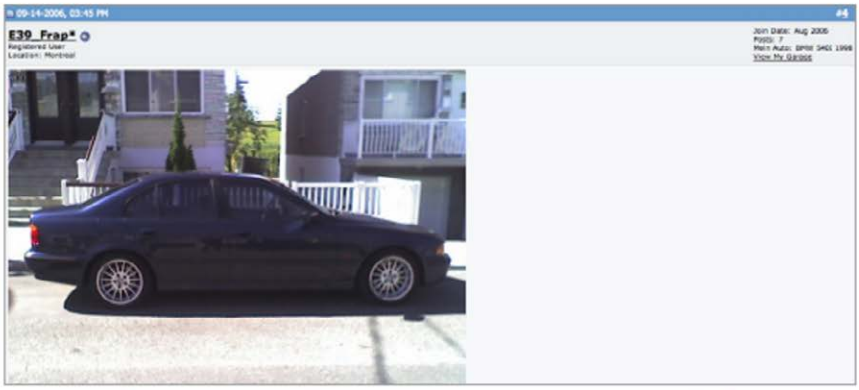

図2：BMW 540i を所有していることを述べた Frapstar のフォーラム上の投稿（クリックすると拡大し

Figure 2—Trend Micro Report on Frapstar

From this report, we learn more key information about the threat actor who goes by Frapstar:

- They have a keen interest in obtaining stolen Canadian credit card accounts
- They own a BMW 5 Series automobile, specifically the E39 540i
- They use the following usernames on various forums:
  - badbullzvenom
  - Badbullz
  - Frapstar
  - Ksensei21
  - E39_Frap* (i.e., E39_Frapstar)

Are There Two Threat Actors Behind the Golden Chickens MaaS?

In the report from Trend, we see that user E39_Frap* self-identifies as "Chuck from Montreal". However, this seems to be at odds with the information from the Exploit.in forum where the threat actor says he is from Moldova and can write in Romanian, as well as in English and French. He even participates in a thread on the Lampeduza forum titled "Romanian only". However, in the earlier thread, we also see where badbullzvenom says he can write in French, which could show a possible connection to Montreal.

Is the threat actor behind the badbullzvenom account from Montreal, Moldova or another Eastern European country where Romanian is spoken? This remained a mystery until we had the opportunity to read through many of the threat actor's older forum posts. Here we found mentions on multiple occasions of the badbullzvenom account being shared between two people. (See Figures 3 and 4).

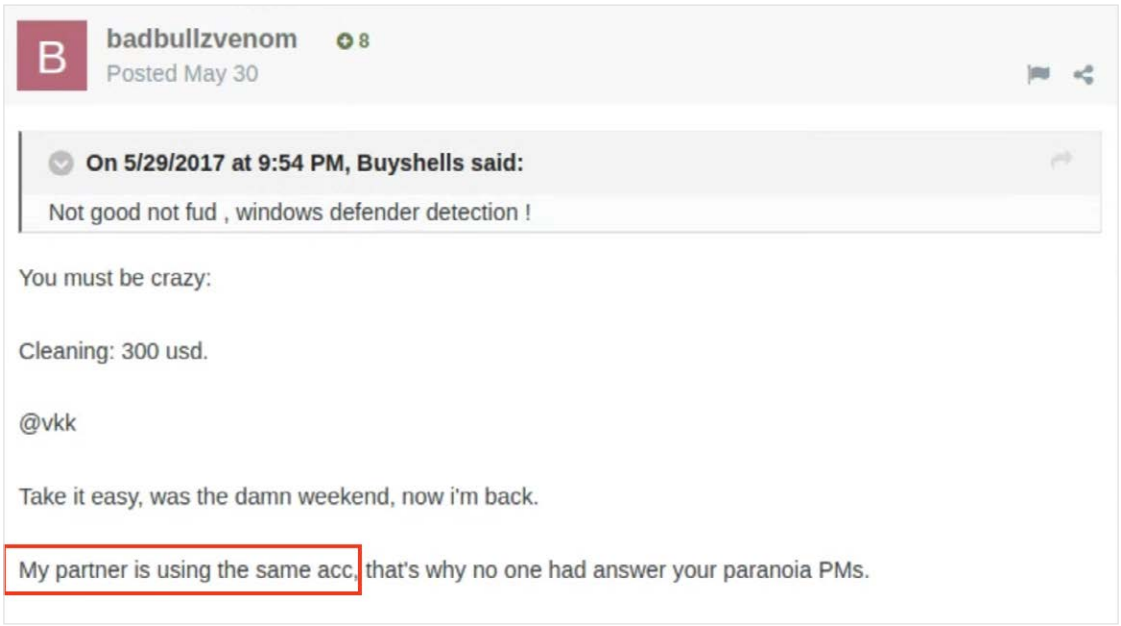

Figure 3—Exploit.in post

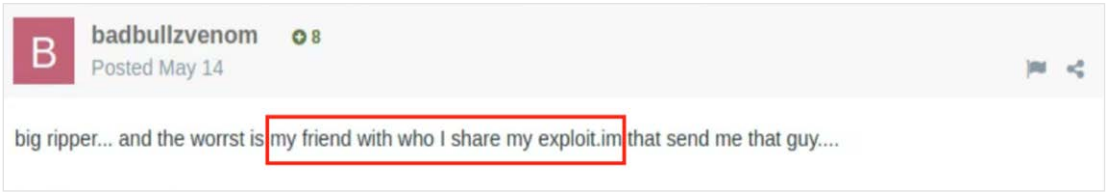

Figure 4—Exploit.in post

TRU believes that "Chuck" is just one threat actor that operates the badbullzvenom account at times, and is in fact located in Montreal, Canada. We also believe there is a second threat actor, possibly from Moldova or Romania, that operates the badbullzvenom account alongside "Chuck."

Timeline of badbullzvenom's Progression from Script Kiddie to MaaS Provider

badbullzvenom's activity on Exploit.in, over the years, demonstrates a progression from a "script kiddie" to a MaaS provider:

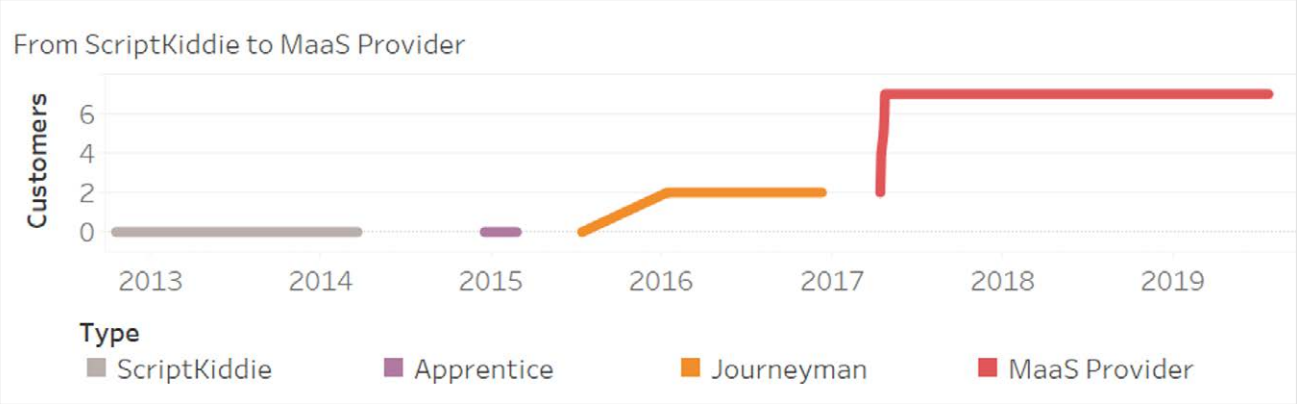

Figure 5—Progression from ScriptKiddie to MaaS Provider

2013 – badbullzvenom first recorded posts on the forum that are often complaints about other users. He demonstrates an interest in Canadian computer traffic and Canadian banks such as TD, CIBC, Scotiabank, and BMO.

2014 – Throughout the majority of 2014, badbullzvenom only posts three times in Exploit.in.

2015 – badbullzvenom returns from his hiatus, but he tends to demonstrate more confidence and technical acumen. He points other members to appropriate tools of the hacking trade, participates in banter, shows an interest in banking trojans for sale, and starts giving more positive reviews.

2016 – After another hiatus, badbullzvenom returns once again, offering for sale his first cyber tool. He only nets two customers and in this time, he continues to show interest in banking trojans and cryptors, as well as a continued interest in financial data relating to Canada. He also makes aggressive and offensive comments, including one statement he makes before going on hiatus again, where he tells one member of Exploit.in to kill themselves, and he offers to pay for the bullet.

2017-2019 – badbullzvenom returns to the forum once more, offering the sale of "Word 1-day doc builder" – known today as VenomKit. It is a malicious document builder that takes advantage of Windows Office exploits. He accumulates customers quickly and continues to develop the builder, adding new exploits as they appear and updating its features. For example, PowerShell is removed from the attack chain to reduce detection, .dll support is added for payloads, and a .js downloader (likely the more_eggs backdoor component of Golden Chickens is added and is for sale.) During this timeframe, Cobalt Group **is reported** as using badbullzvenom's builder to deploy Cobalt Strike in attacks on banks – then **again in 2018**. In 2019, **FIN6 is observed** using more_eggs with employment lures.

Picking Up The Trail

In recent years, database leaks have exposed billions of users' credentials, leading to hacking and privacy concerns. However, one aspect of this activity works in favor of network defenders – the fact that numerous hacking forums have had their user databases leaked, offering an opportunity to make connections between online personas of known threat actors and their real-world identities.

Referencing the 2015 Trend Micro report, we confirmed the threat actor had accounts in three underground forums. These forums were later breached, and the user databases leaked, revealing email addresses used by the threat actor in the past:

- Carder.pro
  - frapstar:newmoneystink@safe-mail.net
- Opensc.ws
  - ksensei:newmoneystink@safe-mail.net
- Carder.su
  - frapstar:frapstar@safe-mail.net

Other database leaks revealed an account using the newmoneystink@safe-mail.net email address with the password "Nay45uck+". Pivoting on this piece of information leads us to an old Myspace account registered to dalion67@hotmail.com that used the same password. While it is possible there could be two users that coincidentally chose the same rather unique password, searching Google leads us to the account "crazyteg67" on the Montreal Racing forum using that email address, to sell $1000 worth of gift cards for $700.

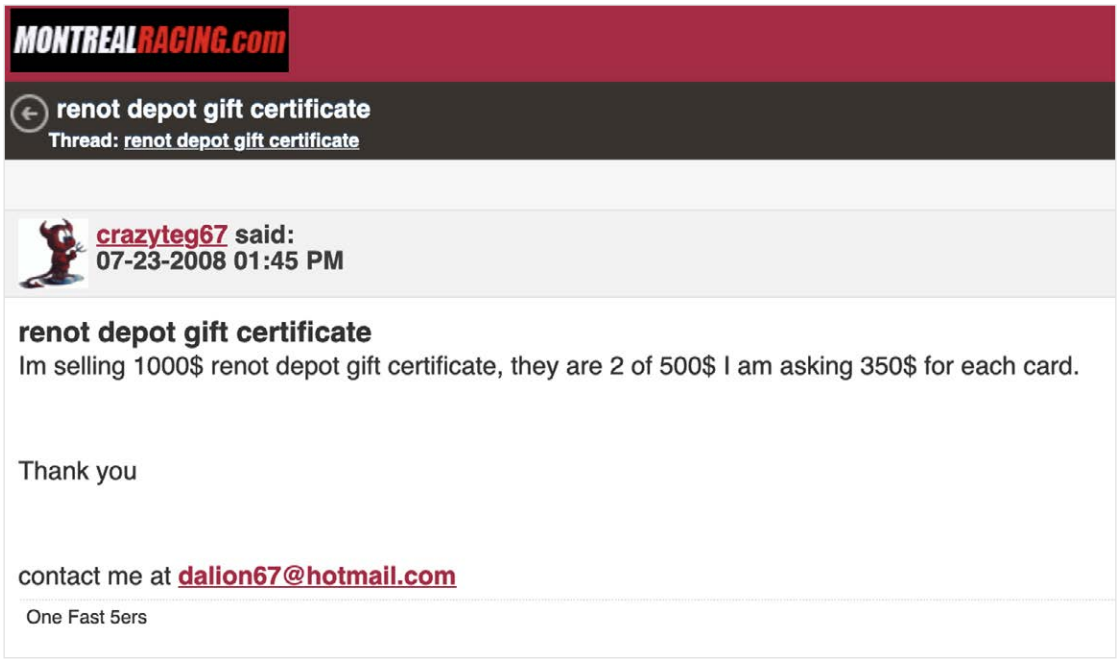

Figure 6—Montreal Racing Post

This account seems to be shared by multiple people, as there are frequent posts offering items for sale with different contact phone numbers and first names in the offer. One of the contact names is "Chuck".

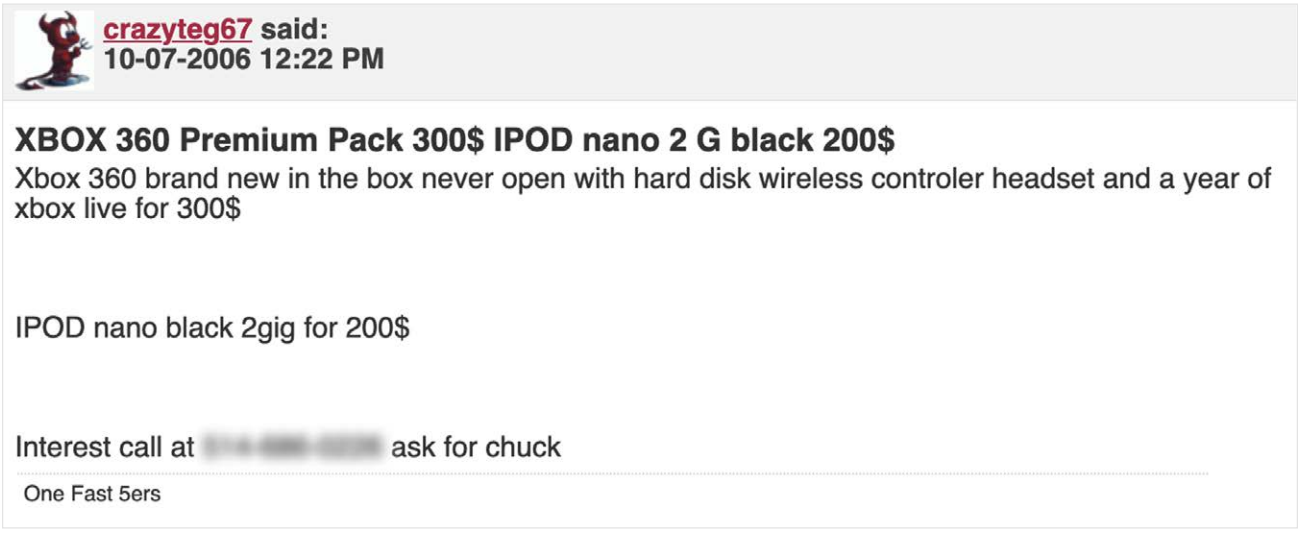

Figure 7—crazyteg67 selling an XBOX 360 as "chuck"

The crazyteg67 user also owns a BMW 540i according to his own posts:

Figure 8—crazyteg67 looking for a 540i clutch replacement

The Social Media Trail

Pivoting on the "dalion67" username, we find a Pinterest account for "Dee Inconegro", with a few boards created under it. One of those boards is dedicated to BMW M5 series photos, and another is dedicated to photos of English Bull Terriers, and the name of the board is "Bad Bullz".

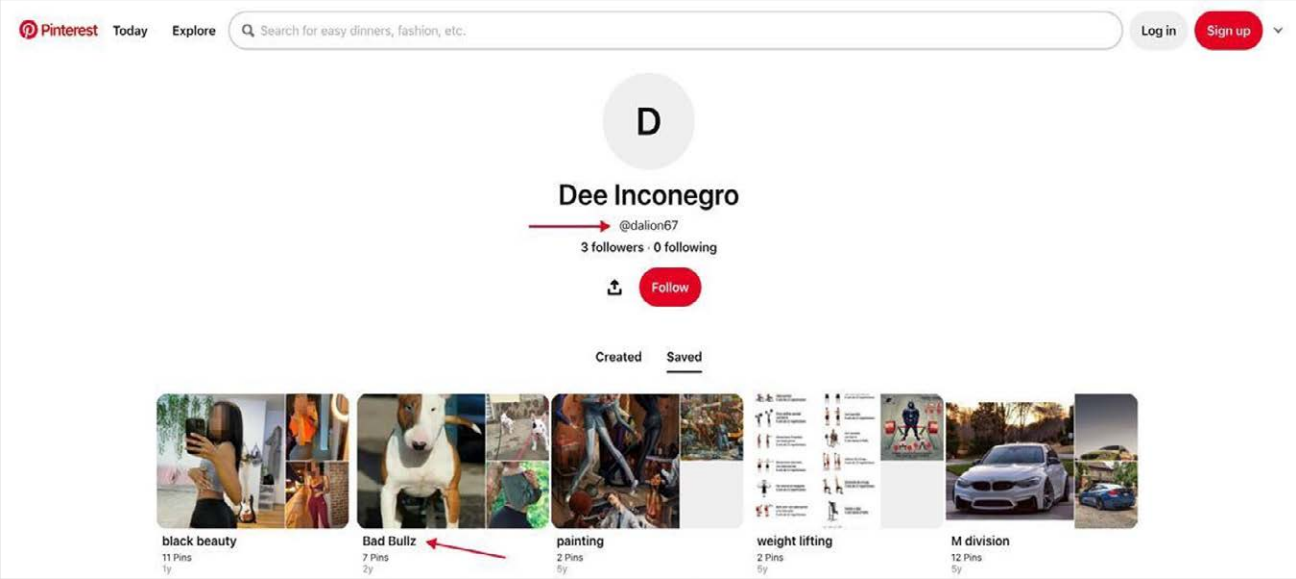

Figure 9—Pinterest profile

Interestingly, there is a Facebook account using the same fake name "Dee Inconegro", with only a few posts. However, we can see references to this account in other users' posts, one of which referred to the account by an older name, "Keyser Sensei" (See Figure 11), which we found amusing as it appears to be a reference to the mysterious crime lord character—Keyser Söze in the movie, Usual Suspects.

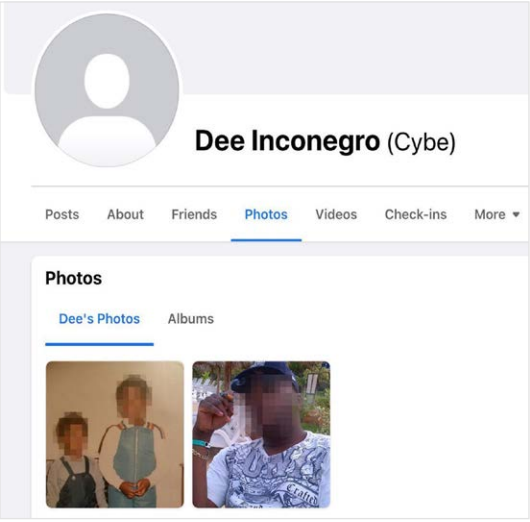

Figure 10—Dee Inconegro Facebook profile

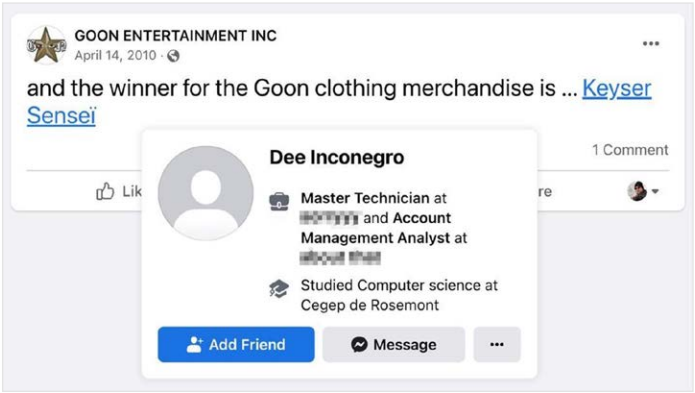

Figure 11—Facebook post linking to Dee Inconegro profile

Additionally, this account is linked through multiple friends to another account with the name "Chuck Larock", which appears to be an older account of the same actor, where he shared photos of his English Bull Terriers. However, this name is also an alias, not the real name of the threat actor.

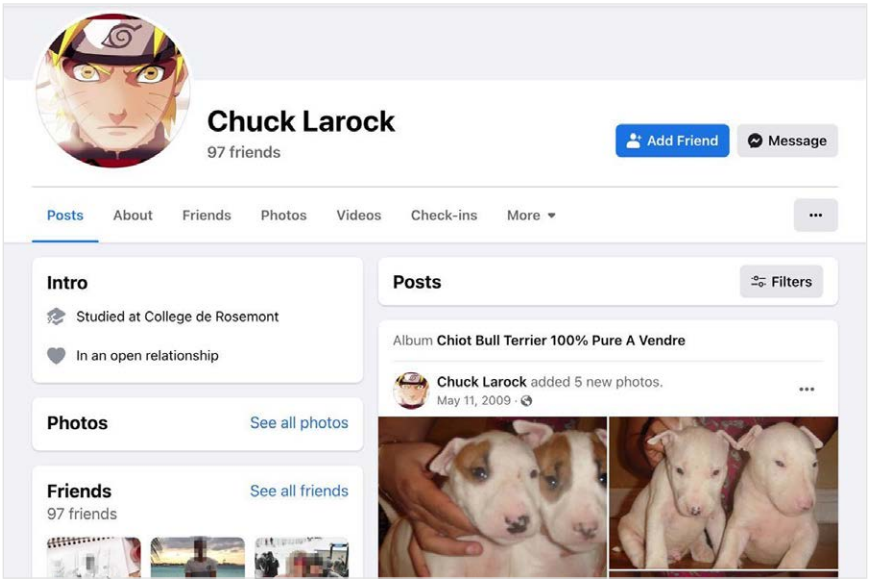

Figure 12—Chuck Larock Facebook profile

Even though the threat actor is careful to never use his real name when creating social media or forum accounts, a comment from one of "Chuck Larock's" Facebook friends gives us a clue.

Figure 13—Facebook comment

The comment, where a friend says: "yo [name redacted] ca va" which casually means "hey, how are you?" in French. This might easily be overlooked, because the name the friend calls out in the comment is not a common name and not meaningful by itself. However, in the context of Dee Inconegro's Facebook page, we find another clue. From public records, we learn that Dee Inconegro's listed employer, [company name redacted.ca], is actually owned by a man who goes by [name redacted], a Canadian citizen of Haitian descent.

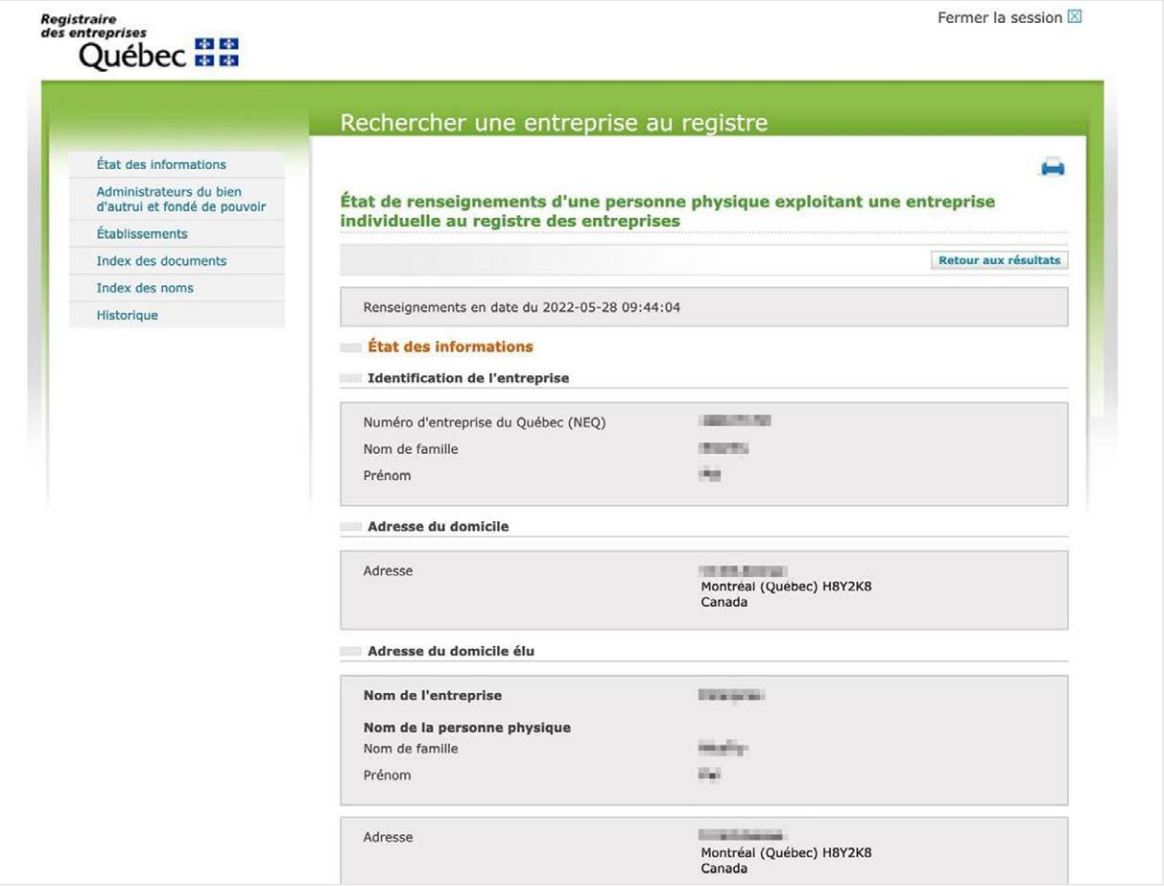

Figure 14—Business registration for [company name redacted]

It appears that [company name redacted.ca] is a sole-proprietor business, operated from a residential address in Montreal. One former Google Street View photo shows an image of the location with two BMWs in the driveway and a person (possibly our threat actor) standing in front.

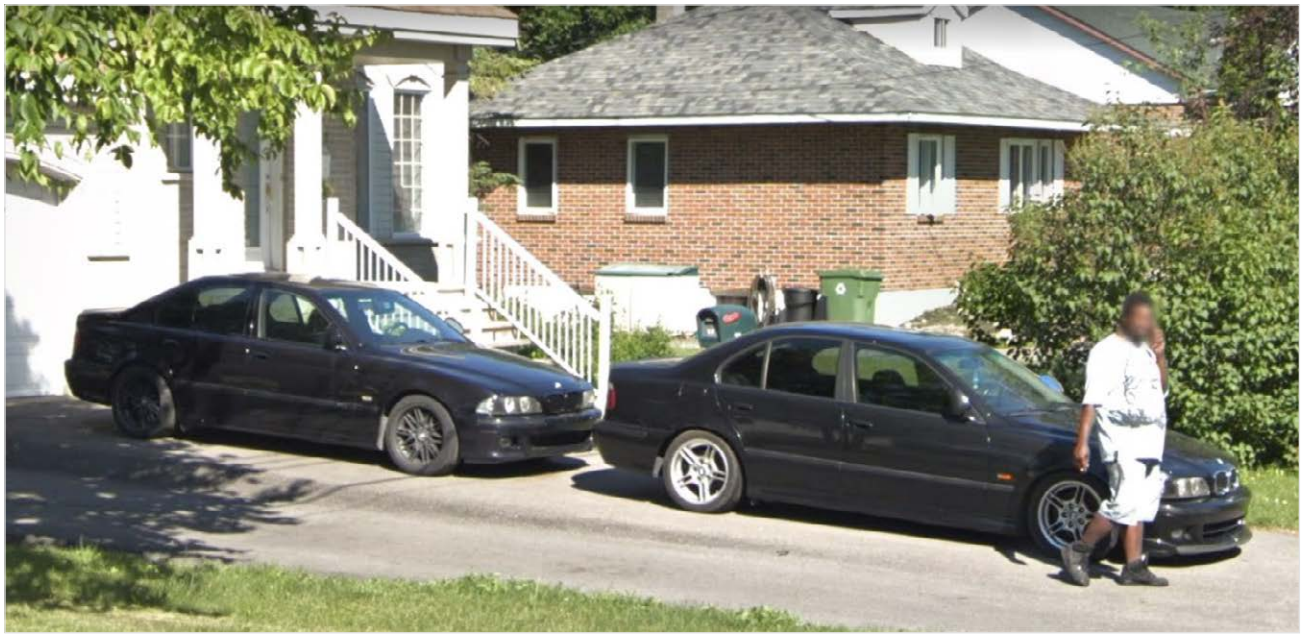

Figure 15—Google Street View image of [name redacted.ca] office

This name matches another email address posted by the account on the Montreal Racing forums, [name redacted]@sympatico.ca.

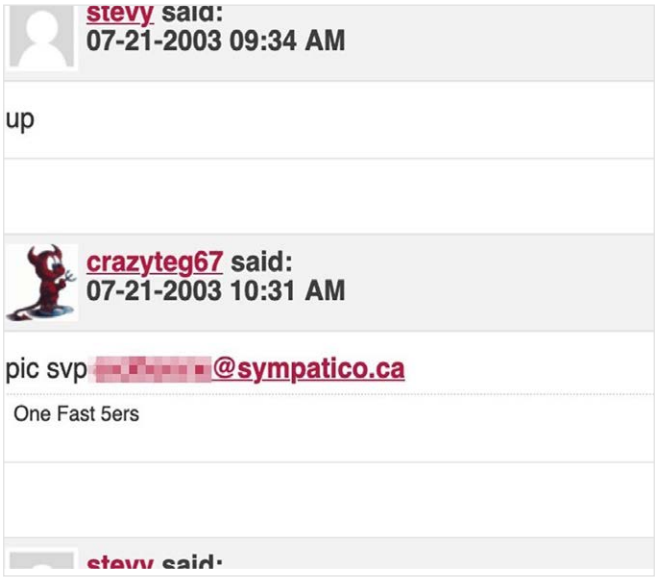

Figure 16—crazyteg67 asking for photo

References to the number "67" in usernames used by the threat actor and his associates could suggest an affiliation with the **Montreal 67s**, a Haitian street gang.

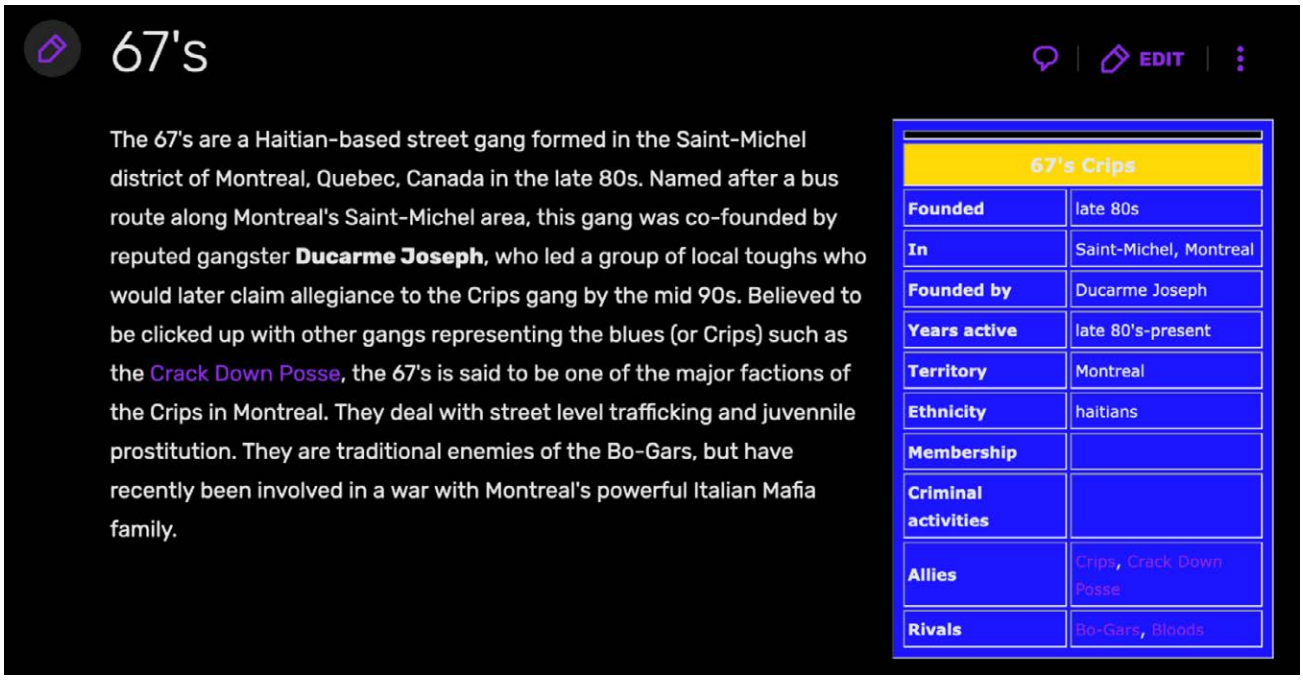

Figure 17—Background information on the 67's street gang

About the Golden Chickens Malware Suite—a Modular Malware

Golden Chickens is a stealthy, highly functional, all-in-one suite of malware. It consists of various components that threat actors can select for their objectives:

More_eggs – This is the Golden Chickens' key component. More_eggs provides threat actors with a back door and a malware loader.

VenomLNK – Initial access for more_eggs. VenomLNK is a .lnk file (Windows shortcut) sent to victims to instigate User Execution.

TerraLoader – The primary goal of VenomLNK is to instantiate TerraLoader which can then load the individual objective-based plugins.

TerraRecon – Performs initial environmental analysis of the infected machine and provides threat actors with some rudimentary information of the organization's network.

TerraStealer – Harvests credentials and emails from browsers, email clients, and transfer utilities.

TerraTV – Allows threat actors to move laterally in the network by hijacking the organization's running instance of TeamViewer.

TerraPreter – Provides a meterpreter shell that allows threat actors to perform actions such as lateral movement, discovery, and credential theft manually.

TerraCrypt – An encryption payload for ransomware extortion attacks.

TRU Detects a New Golden Chickens Campaign & E-Commerce Companies Appear to Be the Targets

Since the beginning of 2022, TRU has observed several incidents in which VenomLNK, a .lnk file (a Windows shortcut) sent to victims to instigate User Execution, was leveraged to target corporate hiring managers in the U.S. A single sample uploaded to VirusTotal in July 2022, from France, pointed to a new resume-themed download server, suggesting ongoing cyberattacks utilizing Golden Chickens. The associated URL indicates the malware is being used to go after e-Commerce companies, which we know is a favorite target of FIN6, the financial crime group known for successfully compromising large e-Commerce companies including British Airways, Newegg, Ticketmaster and countless others.

In order to deliver VenomLNK to victims and ensure that they click on them, the Golden Chickens operators leverage employee recruitment processes. The threat actors engage targets through services such as LinkedIn, Indeed, and the organization's own careers section of their website. In the past, operators started by engaging the victim on LinkedIn, eventually following up with a job offer through email.

In the July campaign, VenomLNK is hosted on a personal branding web page (See Figures 18 and 19). The operators then send a link leading to a mock resume PDF through the organization's recruitment platform (e.g. Indeed, LinkedIn, or the organization's own career web page). The PDF purports to be broken, offering an embedded link (Figure 20) to the malicious VenomLNK file on the branding website, which the victim then downloads and executes manually after completing a CAPTCHA.

Figure 18—The landing page of the personal branding website hosting VenomLNK

Figure 19—Personal branding website hosting VenomLNK

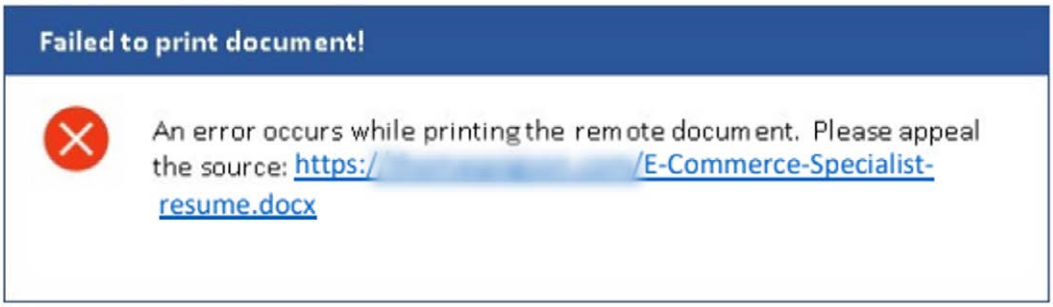

Figure 20—The only content in the PDF is a fake error message with a link directing the victim to download VenomLNK

Using a CAPTCHA on a website makes it harder for security researchers and their tools, especially if those tools are automated, to retrieve and analyze if there is any malware present. Evasion tactics, like this, are a clever way for threat actors trying to get a foothold into an e-Commerce company to increase their chances of success.

A $200,000 Bounty Issued for badbullzvenom on July 18, 2022

Not only has TRU detected what appears to be a new Golden Chickens attack campaign, but on July 18, 2022, a threat actor going by "babay" went on to Exploit.in and accused badbullzvenom of stealing $1 million from him. Consequently, babay issued a $200,000 bounty for any information leading to badbullzvenom's real identity. See Figure 21.

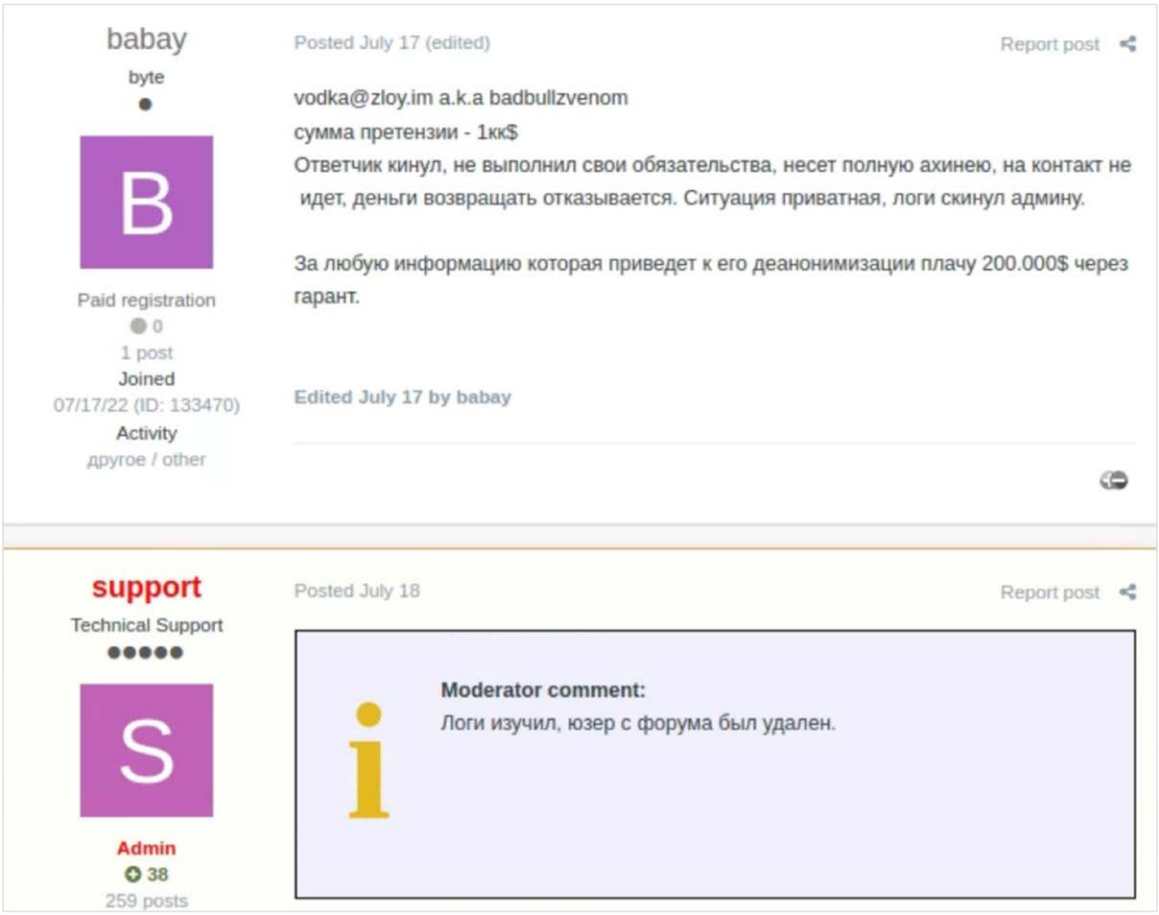

Figure 21—A threat actor on Exploit.in accuses badbullzvenom of stealing $1 million from him and offers a $200,000 bounty for any information leading to badbullzvenom's real identity

The translation of the complaint made on July 18, 2022 by babay about badbullzvenom in Exploit.in:

"vodka@zloy.im a.k.a. badbullzvenom
The total cost of the complaint $1,000,000.
The person scammed me, didn't complete his job, talk total nonsense, I can't contact him and he refuses to return the money back. The situation is private, I sent the logs to the admin.

For the information that can lead to his deanonymization I will pay $200,000 through the guarantor."

The translation of Exploit.in's Administrator/Moderator's response to babay:

"I have looked through the logs, the user is deleted from the forum."

The Significance of Discovering the Identity of the Golden Chickens Operator

1. **The connection to The Billion Dollar Hackers:** The Golden Chickens MaaS is a favorite cyber weapon of three of the longest-running and successful financial crime gangs on the Underground: Russia-based FIN6 and Cobalt Group, and Evilnum, a hacker group suspected to operate out of Belarus, a neighbor and ally of Russia. In learning more about the threat actor behind Golden Chickens and understanding his operation, TRU can garner more intelligence about the TTPs of the FIN6, Cobalt Group and Evilnum operations. This knowledge is invaluable for eSentire and other cyber defenders, as they develop security protections that will detect, respond and shut down attacks launched by these threat groups.

2. **Collaboration with Law Enforcement:** In 2015, the Trend Micro report about Frapstar, aka badbullzvenom, provided solid intelligence about this threat actor, giving law enforcement a real chance of identifying and potentially arresting badbullzvenom when he was still a minor player on the cybercrime scene. Instead, he has had seven years to hone his skills, and from our findings, we see that he has continued to get better at developing malware and obfuscating it. badbullzvenom is very stealthy, and he goes to extremes to keep his malware fully undetectable (FUD) by anti-virus, trying to make sure that samples of Golden Chickens are not uploaded to VirusTotal. badbullzvenom also insists that his clients ONLY use his malware in very "targeted" attacks to further ensure that he and his malicious software fly under the radar.

   We believe the case of the Golden Chickens operator is a stark example of what can happen if a threat actor, who is considered "low hanging fruit," is ignored by law enforcement. All eSentire's research has been transitioned to law enforcement for criminal investigations.

3. **Understanding Golden Chickens Malware:** Discovering the identity and activities of the Golden Chickens operator has enabled Stewart and Keplinger to answer several questions about the malware suite, such as:
   a. Why do security researchers see so few hacker campaigns involving the Golden Chickens malware?
   b. How long has badbullzvenom been conducting cyber fraud?
   c. What TTPs does badbullzvenom use to avoid detection?

Conclusion

There is compelling evidence that the threat actor, detailed in this report, is one of possibly two operators behind the badbullzvenom account on Exploit.in.

Interestingly, as of July 2022, all of badbullzvenom's posts on Exploit.in have been purged from the forum.

However, TRU continues to see improvements in the Golden Chickens source code and new Golden Chickens attack campaigns, like the one we detected in July. That tells us that the malware suite is still actively being developed and is being and sold to other threat actors. We expect to see further targeted attacks against financial institutions and organizations, processing large amounts of credit and debit card data, leveraging this malware in the foreseeable future. Thus, TRU is continuing to investigate the Golden Chickens operation and any other parties that may be involved.

It is TRU's recommendation that organizations take the following steps to protect against the Golden Chickens malware suite:

1. Employ exhaustive endpoint monitoring for LOLBINs, aka **Trusted Windows Binary abuse**. LOLBINs of interest include cmd.exe, wscript.exe, wmic.exe, cmstp.exe, msxsl.exe, powershell.exe, and ie4uinit.exe. Ensure endpoint products have rules in place to detect suspicious usage of these Windows processes.

2. Ensure employees are aware of common phishing tactics:
   a. Be suspicious of attachments from people you don't know – additional care is required in cases where you must accept documents from the public (such as with employee hiring process)
   b. Inspect attachment file types by right clicking the file and selecting properties
   c. Documents should never come as LNK, ISO, or VBS files
   d. Often, these malicious files will be enclosed in a .zip file to bypass email filters

3. Have an easy process in place for reporting phishing and suspicious behavior
   a. Leadership is responsible for ensuring a positive and convenient path is in place for reporting suspicious behavior
   b. Develop a collaborative culture of cyber resiliency where employees are comfortable to bring forward questions, and even mistakes when it comes to email behavior and downloads. Punishing employees for falling for phishing scams will reduce the chances that they – and other employees – report them in the future.

4. Engage Managed Detection and Response services for 24/7 Security Monitoring, Threat Hunting and Threat Containment expertise. The speed with which you can detect and contain a threat actor before they achieve their objectives is imperative in preventing business disruption.

Indicators of Compromise (IOCs)

Domains

johnwagen[.]com
mikelatona[.]com
liamelston[.]com
mikegarmon[.]com
robertbuss[.]com
johncheston[.]com
jamesstepleton[.]com
jamesreuther[.]com
williamhankins[.]com
jamesdabill[.]com

VenomLNK SHA256

33e5078833aa2caf7dcbae23300c6a4635076625e79f2368871727e895e76d89
05d9e8a947dbaebb6c3df9889bc2db55f1ba58f18f16a96d105bf9f3438081bb
26fdd198192575716c72f1cc08c6ad0f9828d5bb90225436caf654b95c967ee3
ce08dbf119fbe2effdecce7374bb12b2720489a6508bef67f1d297b25fceeadf
c8fe70f61d05b50dd5f9000979f517e2e9a89b6f9d3e8d896af82064de187cb7
c611088c624895be4e347e0d474405a2ddf582af0172867014666d5a78e657dc
7d3bbf055179fb53d7ffcbb0c0a2c07caea64c5bdc5db442d8babba8da398abf