FIN7 Recruits Talent For Push Into Ransomware

geminiadvisory.io/fin7-ransomware-bastion-secure

October 21, 2021

The intelligence in this report was gathered by a source who was recruited by "Bastion Secure". Gemini Advisory's investigation and analysis of the source's information has been ongoing for the past several months. Although sensitive information has been redacted from this report to protect the source, Gemini Advisory has provided law enforcement with the complete set of unredacted information. In addition, our findings were reported to our clients earlier this month and have been corroborated by Microsoft's presentation at Mandiant Cyber Defense Summit 2021.

Key Findings

- The cybercriminal group FIN7 has been responsible for large-scale card theft campaigns, resulting in the exposure of over 20 million payment card records, as well as ransomware attacks. Gemini has discovered that FIN7 is now running a new fake company called "Bastion Secure", replacing the previously reported "Combi Security".

- Bastion Secure offered a job offer to a Gemini source and, in the process, provided the source with files that analysts later determined were for the post-exploitation tools Carbanak and Lizar/Tirion. These two tools have been previously attributed to FIN7 and establish the link between Bastion Secure and FIN7.
- The tasks that were assigned to the Gemini source by FIN7—operating under the guise of Bastion Secure—matched the steps taken to prepare a ransomware attack, providing further evidence that FIN7 has continued to expand into the ransomware sphere.
- FIN7 can pay unwitting "employees" far less than it would have to pay informed criminal accomplices for its ransomware schemes. However, FIN7's greed also afforded Gemini a view into the proprietary data of this prolific threat team, leading to the exposure of another fake FIN7 company.

Background

The cybercriminal group FIN7 gained notoriety in the mid-2010s for large-scale malware campaigns targeting the point-of-sale (POS) systems. In 2018, Gemini Advisory reported FIN7's compromise of Saks Fifth Avenue and Lord & Taylor stores and the subsequent sale of over 5 million payment cards on the dark web. According to the US Department of Justice, the broader FIN7 carding campaigns have resulted in the theft of over 20 million payment card records and cost victims over $1 billion, making FIN7 one of the most infamous and prolific cybercriminal groups of the last decade. Now with ransomware proving to be cybercriminals' preferred high-profit, jackpot venture, FIN7 has redeployed their expertise and capacity towards ransomware, with reports indicating that the group was involved in attempted ransomware attacks on US companies as early as 2020. Furthermore, despite focus from law enforcement and the arrest of four FIN7 members from 2018 to 2020, FIN7's continued activity shows that the group remains a powerful, active threat.

In 2018, the US Department of Justice revealed that FIN7 was posing as "Combi Security", a fake cybersecurity company, to involve unaware IT specialists in their carding campaigns. While the public focus on Combi Security shut down that operation, Gemini has now discovered that FIN7 is using a new fake cybersecurity company named "Bastion Secure" to lure unaware IT specialists into supporting its continued expansion into ransomware.

Over the course of FIN7's existence, cybersecurity firms have referred to FIN7 by several names—including Carbanak, Carbon Spider, Anunak, Cobalt Gang, and Navigator Group—with some practitioners choosing to subdivide the FIN7 designation according to the target type. While overlapping but different groups of individuals have likely conducted malicious activity attributed to these threat groups, the unifying thread connecting the attack signatures to FIN7 has been the use of the malware Carbanak.

Analysis

A Gemini source was offered a position as an IT specialist at “Bastion Secure Ltd”, a cybersecurity “company” seeking C++, Python, and PHP programmers, system administrators, and reverse engineers. A basic search for this company returns a legitimate-appearing website (www[.]bastionsecure[.]com), but analysis revealed that it is a fictitious cybersecurity company run by a cybercriminal group. During the interview process, the source was given several tools for test assignments that the source would use if employed.

Gemini Advisory worked jointly with the Recorded Future Insikt Group to analyze the tools provided by Bastion Secure and determined that they are actually components of the post-exploitation toolkits Carbanak and Lizar/Tirion, both of which have been previously attributed to the FIN7 group and can be used for both POS system infections and ransomware attacks.

Prior to 2020, FIN7’s primary modus operandi was to compromise companies’ networks and infect POS systems with credit card-stealing malware. Since 2020, cybersecurity researchers have identified instances in which FIN7 gained access to company networks that were later infected with either REvil or Ryuk ransomware. FIN7’s exact involvement in the deployment of ransomware—i.e., whether they sold the access to ransomware groups or have formed a partnership with these groups—remains unclear. However, the tasks that were assigned to the Gemini source by FIN7 (operating under the guise of Bastion Secure) matched the steps taken to prepare a ransomware attack, providing further evidence that FIN7 has expanded into the ransomware sphere.

Furthermore, due to Bastion Secure’s use of Carbanak and Lizar/Tirion and FIN7’s established practice of using fake cybersecurity companies to recruit talent, Gemini assesses with high confidence that FIN7 is using the fictitious company Bastion Secure to recruit unwitting IT specialists into participating in ransomware attacks.

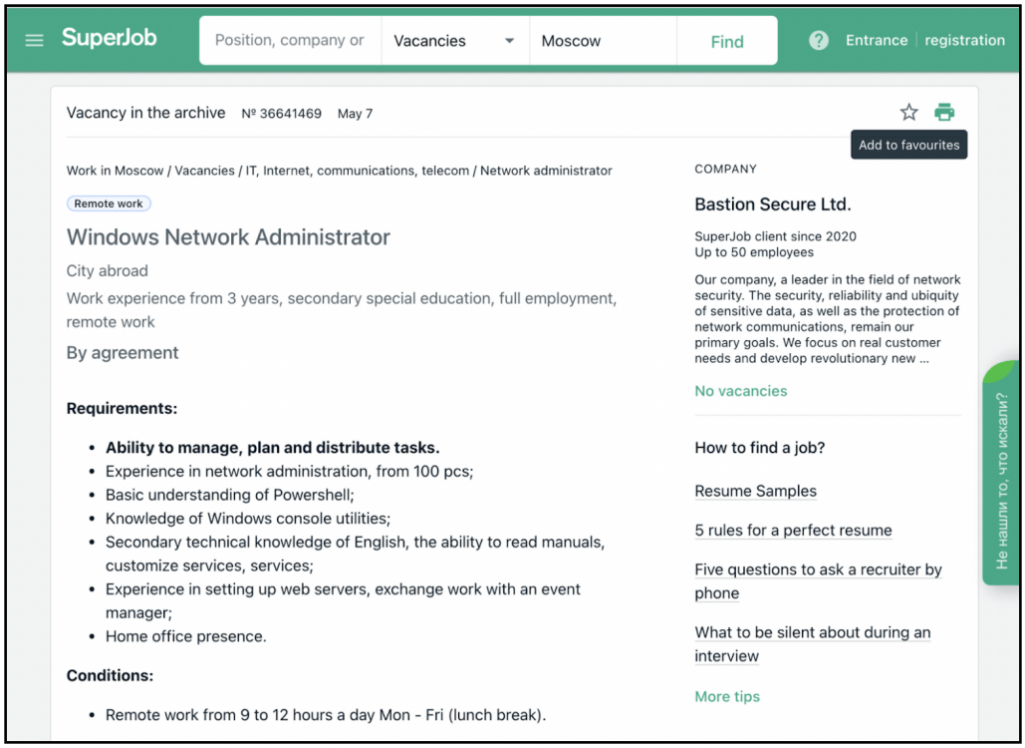


Image 1: Bastion Secure posts a job offer for a Windows Network Administrator on the Russian job site superjob.ru.

More broadly, FIN7's decision to use a fake cybersecurity company to recruit IT specialists for its criminal activity is driven by FIN7's desire for comparatively cheap, skilled labor. Bastion Secure's job offers for IT specialist positions ranged between $800 and $1,200 USD a month, which is a viable starting salary for this type of position in post-Soviet states. However, this "salary" would be a small fraction of a cybercriminal's portion of the criminal profits from a successful ransomware extortion or large-scale payment card-stealing operation. In effect, FIN7's fake company scheme enables the operators of FIN7 to obtain the talent that the group needs to carry out its criminal activities, while simultaneously retaining a larger share of the profits.

FIN7's use of Bastion Secure—even after the discovery of Combi Security, the group's previous fake cybersecurity company—indicates that FIN7 continues to believe that hiring unwitting IT specialists is the group's best method for balancing the need for a technically skilled team against the operators' desire for maximum profits.

Bastion Secure

With FIN7's latest fake company, Bastion Secure, the criminal group leveraged true, publicly available information from various legitimate cybersecurity companies to create a thin veil of legitimacy around Bastion Secure. In effect, FIN7 is adopting disinformation tactics so that if

a potential hire or interested party were to fact check Bastion Secure, then a cursory search on Google would return “true” information for companies with a similar name or industry to FIN7’s Bastion Secure.

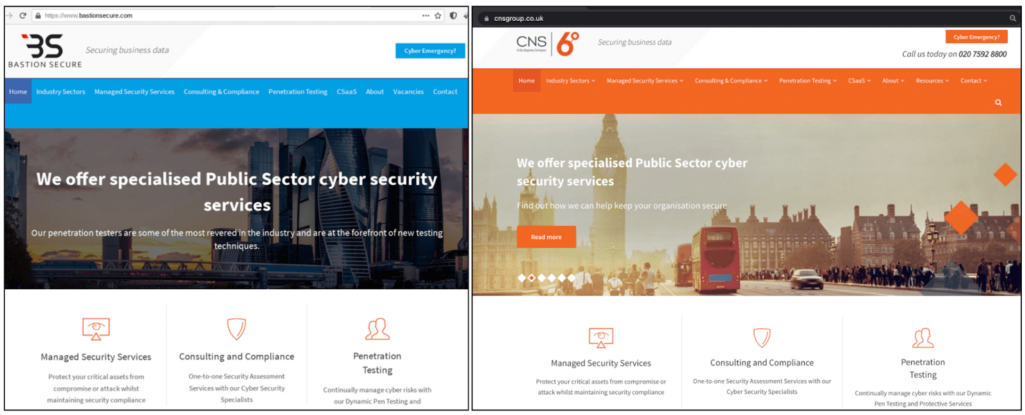
FIN7’s first step in obtaining a veil of legitimacy was to give their fake company the generic name “Bastion Secure”, which appears similar to several unrelated security-adjacent companies with highly listed Google search results:

- Bastion Security Products Ltd: a US physical security company that was recently acquired by ECAMSECURE
- Bastion Security Group: a US physical security consulting company

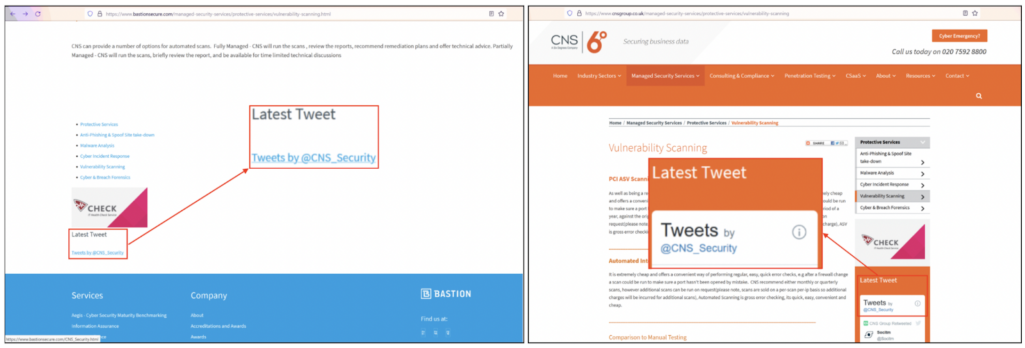
Second, Bastion Secure listed the company’s office addresses as:

- *16e Follingsby Ave, Gateshead, United Kingdom* (former address of the since-closed Bastion Security (North) Limited)
- *94 Yigal Alon St. Tower 1, Tel Aviv, Israel* (office building containing multiple businesses, including the vehicle security company Cymotive)
- *Imperia Tower, 12 Presnenskaya Embankment, Moscow, 123100 Russia* (office building containing multiple businesses). Gemini contacted the Imperia Tower building administrators, who confirmed that there is no company named Bastion Secure with office space at the building.
- *Fortis Tower, 77-79 Gloucester Rd, Wan Chai, Hong Kong* (office building containing multiple businesses). Fortis Tower building administrators did not respond to Gemini’s inquiries; however, public records in the Hong Kong government’s “Companies Registry’s Cyber Search Centre” revealed that there is no registered company named “Bastion Secure” operating in Hong Kong.

Furthermore, the Bastion Secure website itself also appears legitimate at first glance; however, a deeper analysis revealed that the website is largely a copy of the website of Convergent Network Solutions Ltd., a legitimate cybersecurity company. Additionally, the Bastion Secure website is hosted on the Russian domain registrar Beget, which cybercriminals commonly use.



Images 2-3: The website of Bastion Secure (left) is a copy of the website of Convergent Network Solutions Ltd. (right), a legitimate cybersecurity company.



Images 4-5:The Bastion Secure website (left) lists @CNS_Security as its Twitter account, matching the Twitter account listed on CNS' website (right). Additionally, the page description sentence includes text directly from the CNS website.

An initial analysis of the Bastion Secure website revealed that most of the submenus of the site return a Russian-language HTTP 404 error, indicating that the site creators were Russian speakers. Since the initial analysis by Gemini, most of the website's submenus have been fixed with appropriate pages; however, a deeper analysis revealed that some of the HTTP 404 errors remain unfixed.

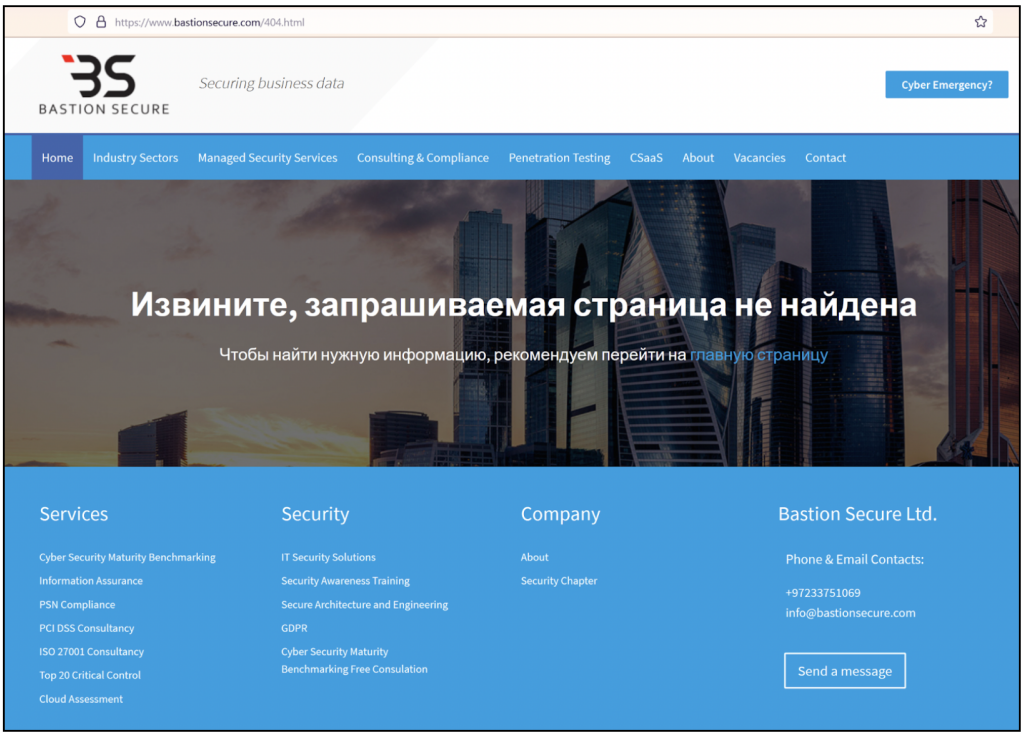


Image 6: Some Bastion Secure pages display a 404 error in Russian, indicating that the site designers are Russian speakers.

As shown in the image below, an analysis of the page's source code reveals the remnants of the CNS site: the code on Bastion Secure still lists the same phone number that is listed prominently on the CNS homepage.

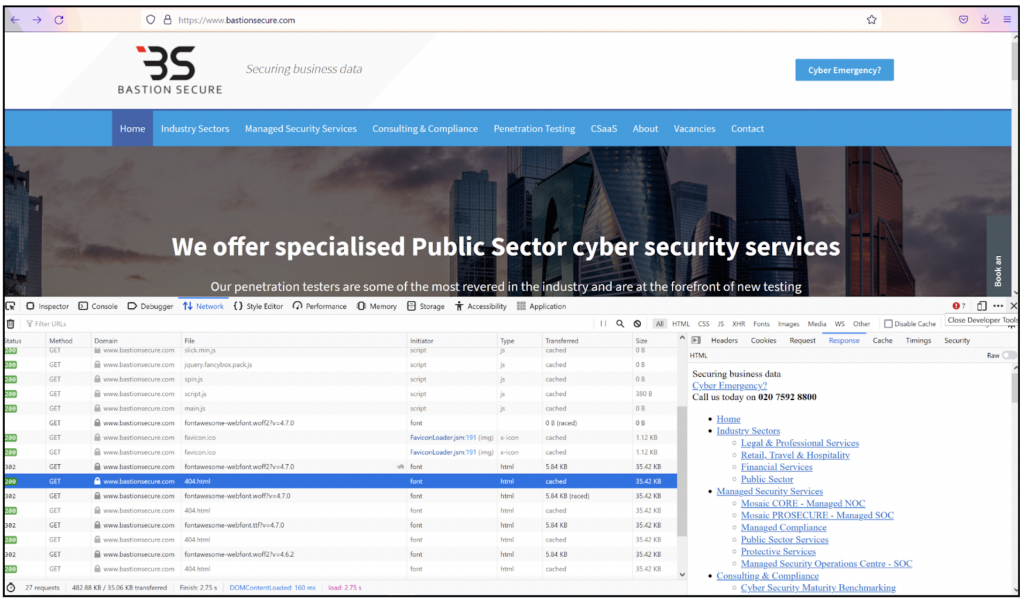


Image 7: The source code under certain pages has been lifted directly from Convergent Network Solutions Ltd's website.

To recruit IT specialists, Bastion Secure posts legitimate-appearing job offers on both their website and prominent job search sites in post-Soviet states, as well as providing reputable-looking contacts to potential hires for additional credibility. In the past several months, Bastion Secure has posted job offerings for system administrators on job search sites and added new vacancies for PHP, Python, and C++ programmers and reverse engineers on their website. On these job sites, Bastion Secure provides sufficiently professional information to appear legitimate and includes purported office information and a phone number (+7 499-642-3420). The list of legitimate Russian and Ukrainian job sites where Bastion Secure has a presence and has advertised job postings includes:

- https://www.superjob.ru/vakansii/administrator-windows-setej-36641469.html
- https://ua.joblum.com/company/bastion-secure-ltd
- https://ua.jubee.org/ru/company/bastion-secure-ltd
- https://rabota.ua/company10418701
- https://jobs.ua/company-bastion-secure-ltd-1603731
- https://moscow.cataloxy.ru/firms/bastionsecure.com.htm – 74996423420
- https://remoteworkukraine.com/ua/company/ua-bastion-secure/

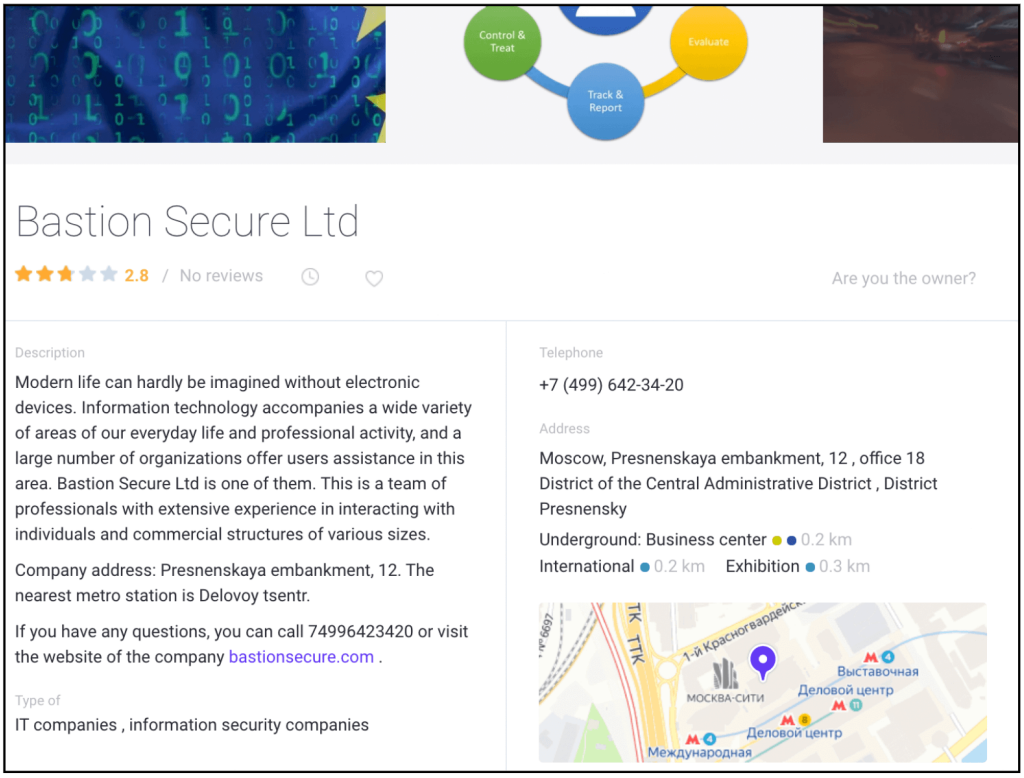
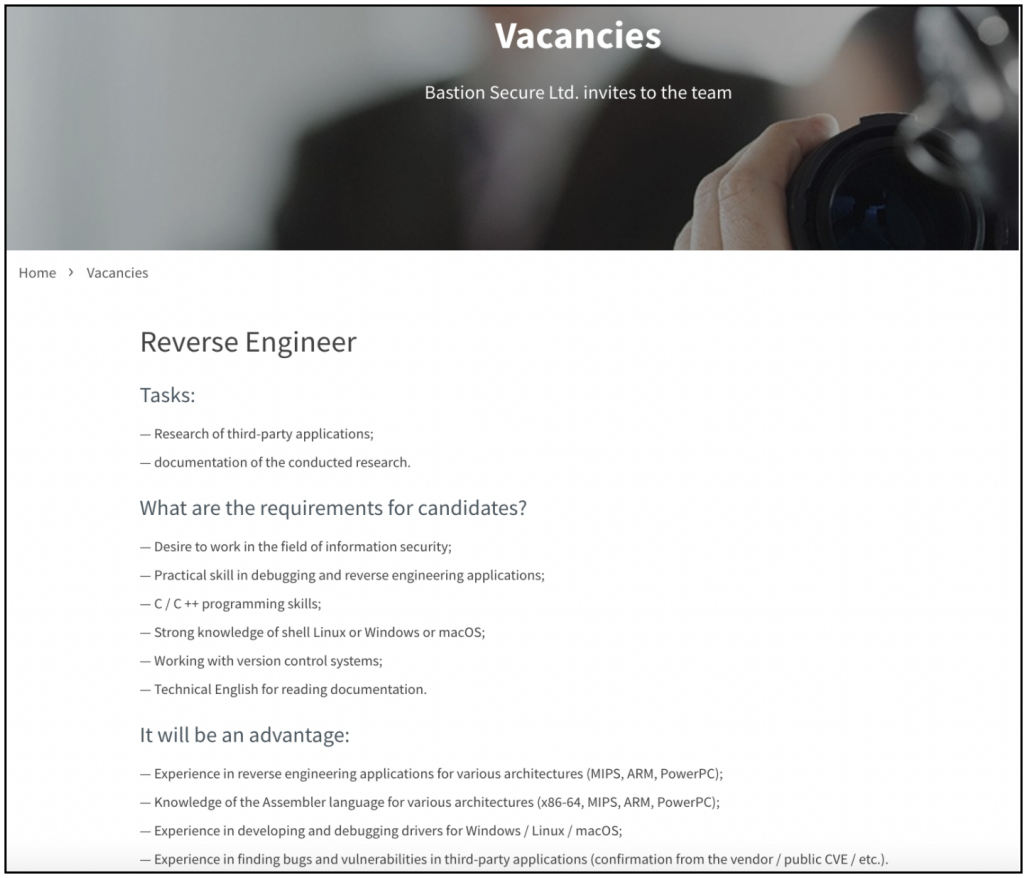


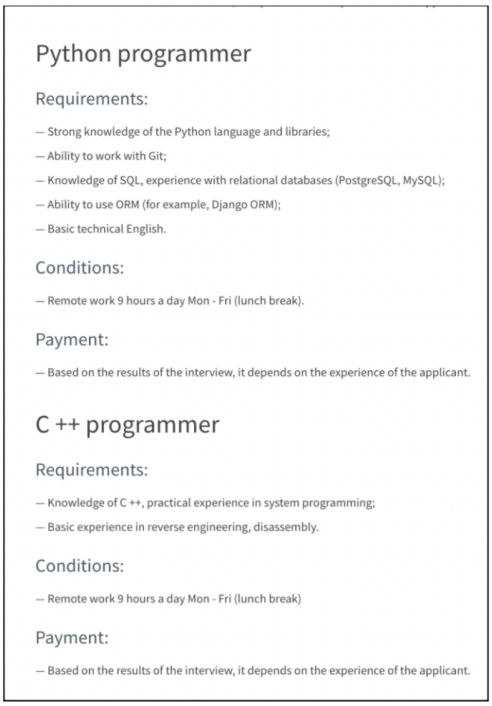
Image 8: Bastion Secure's company page on zoon.ru, a business development site serving Russian companies, job seekers, and consumers.

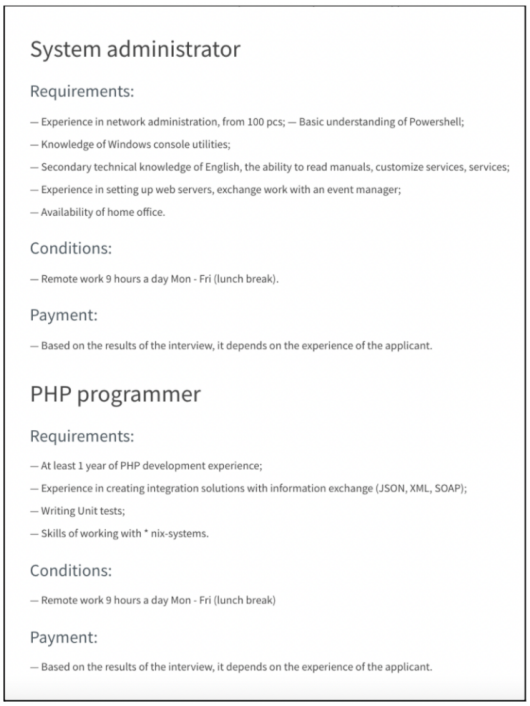
FIN7—operating under the guise of Bastion Secure—is looking for programmers (PHP, C++, Python), system administrators, and reverse engineers in order to build a "staff" capable of conducting the tasks necessary for undertaking a range of cybercriminal activity. Given FIN7's increased interest in ransomware, Bastion Secure is likely specifically looking for system administrators because an individual with this skill set would be able to:

- Map out compromised companies' systems
- Identify users and devices within the systems
- Locate backup servers and files

In order for the system administrator to map out a victim's system, FIN7 would need to first provide the individual with access to the system. FIN7 operators could obtain the initial access through their well-documented phishing and social engineering methods or by purchasing access on dark web forums from a large pool of vendors. Once the system administrator mapped out the system and identified backups, FIN7 could then escalate to the next step in the malware and ransomware infection process. Gemini Advisory has previously written reports on how ransomware teams operate and some of their TTP's.







Images 9-11: Bastion Secure posts job vacancies for IT specialists on its website.

FIN7's Bastion Secure Reveals Criminality During Hiring Process

A Gemini source made contact with a Bastion Secure “HR representative” on a job search site, leading to a hiring process in which Bastion Secure shared their business practices and access to several of their tools. Gemini analyzed these tools to discover that they were in fact the post-exploitation tools Carbanak and Lizar/Tirion. As various security practitioners have already attributed these tools and ransomware attacks to the FIN7 group, the fact that Bastion Secure representatives provided the source with disguised versions of these attributable post-exploitation tools establishes a strong link between Bastion Secure and FIN7.

First Stage: Interview Process

The first stage of the hiring process proceeded similarly to a legitimate job hiring process and gave no indication that Bastion Secure was a fake company for a cybercriminal group. First, the HR representative from Bastion Secure communicated with the Gemini source and informed them that they had reviewed the source’s resume and were interested in hiring them as an IT specialist.

After the source indicated that they were interested in the position, the source conducted a typical first-stage interview with the HR representative via messages on Telegram. Although many non-criminal individuals in post-Soviet states use Telegram as their preferred messaging app, it is not typical for initial professional correspondences to be conducted on Telegram.

After completing the interviews, the source was informed that they would need to:

- Complete several test assignments before beginning on a probationary basis
- Sign a contract and non-disclosure agreement
- Configure their computer by installing several virtual machines and opening ports

Second Stage: Practice Assignments

At face value, the second stage of the hiring process did not give a clear indication that Bastion Secure is a cybercriminal operation. However, the actions taken later in the third stage clearly made the steps taken in the second stage highly suspicious. The source was instructed to install certain platforms and conduct a series of practice assignments that would be typical for the position.

Bastion Secure also informed the source that they were willing to train new hires in cybersecurity. When the source indicated that they were interested in learning, the company sent them additional files that included tools that could either be used for legitimate penetration testing or malicious activity. Although the tools provided to the source were potentially unusual for the position, Bastion Secure prefaced it by proposing that they would train the source to not only manage client’s systems but also secure them, lending credence to the use of these tools.

Third Stage: “Real” Assignment Signals Criminal Intent

In the third stage, Bastion Secure gave the source their first “real” assignment, and it became immediately clear that the company was involved in criminal activity. The fact that the Bastion Secure representatives were particularly interested in file systems and backups signals that FIN7 was more interested in conducting ransomware attacks than POS infections.

For the first assignment, Bastion Secure provided the Gemini source with a “client company” to work on. The task would have been to use a script to collect information on domain administrators, domain trust relationships, file shares, backups, and hypervisors (the software responsible for creating and running virtual machines). At this point, the source became highly suspicious of Bastion Secure’s activities, noting the following red flags from earlier in the hiring process:

- Bastion Secure provided access to the company’s network without any legal documentation or explanation, suggesting that the access may have been acquired through social engineering or purchased on the dark web
- Bastion Secure was only interested in file systems and backup
- The company warned of a heavy fine if the source installed antivirus software on the virtual machine that they were using
- The employee was required to use specific tools to avoid detection
- Bastion Secure software was purportedly licensed to “Checkpoint Software Inc”, which may have been an attempt to masquerade the software as a product of the legitimate company Check Point Software Technologies Ltd. Security researchers have previously reported that FIN7 has attempted to do this in the past as well.

Attribution

Gemini analyzed the files that were sent to the source by Bastion Secure and found that the files contained components for the post-exploitation tools Carbanak and Lizar/Tirion. Post-exploitation tools—which are part of any ransomware group’s toolkit—allow malicious actors to control infected computers after they have gained initial access to the victim company’s network. Various security practitioners have previously attributed the use of Carbanak and Lizar/Tirion to FIN7. These two factors indicate that FIN7 operators are sharing a partially disguised version of its toolkit with unwitting accomplices through the fake company Bastion Secure.

The files provided to the source by Bastion Secure included files for a software component titled “Command Manager” that was, in fact, a disguised version of the client component of Carbanak (see image 12). Gemini determined this by analyzing the software’s functionality and concluded that it is an updated version of previously identified versions of Carbanak. The main functions of the Carbanak command manager are collecting information about an infected computer and obtaining remote access to the infected computer.

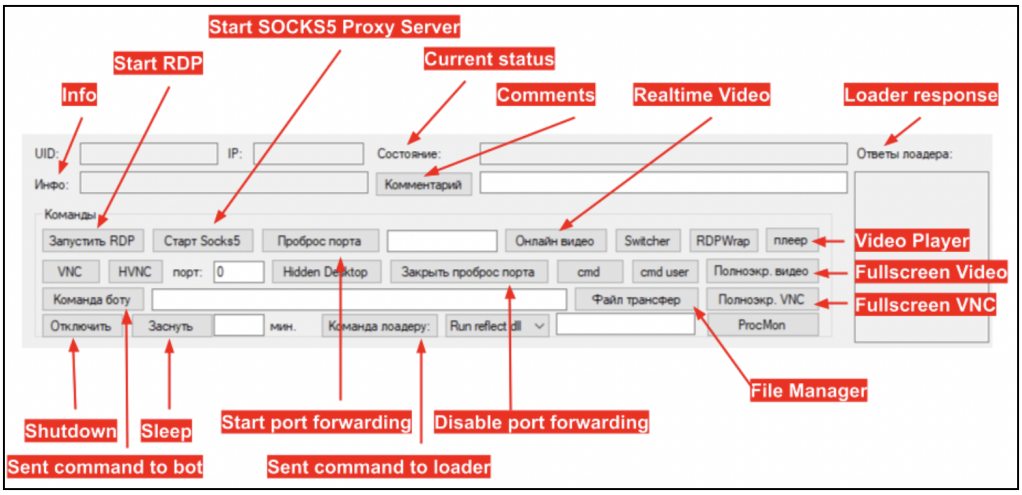


Image 12: Command Manager control panel, which is actually a disguised client component of Carbanak.

The files contained an obfuscated PowerShell script that ultimately launches the Lizar/Tirion injector and payload. The primary function of the loader is to receive periodic commands from the C&C server and execute the commands on the infected computer. The commands executed by the loader on the infected computer are “modules” and the results are sent back to the C&C server. These modules can be .dll, .exe, and .ps1 file types.

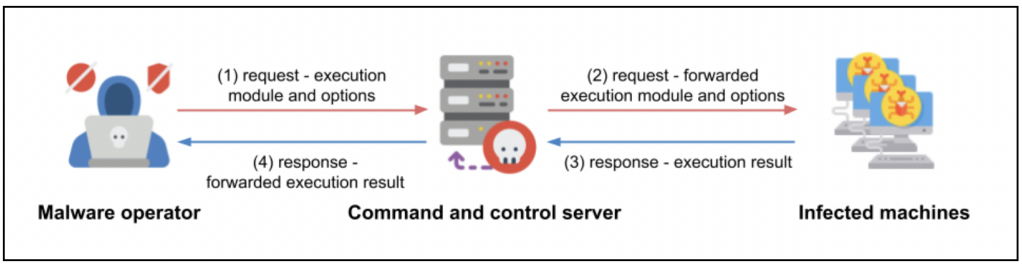


Image 13: The malware operator uses the client to issue commands to the loader, which is located on the infected machine.

Conclusion

Although cybercriminals looking for unwitting accomplices on legitimate job sites is nothing new, the sheer scale and blatancy with which FIN7 operates continue to surpass the behavior shown by other cybercriminal groups. Not only is FIN7 looking for unwitting victims on legitimate job sites, but also attempting to obfuscate its true identity as a prolific cybercriminal and ransomware group by creating a fabricated web presence through a largely legitimate-appearing website, professional job postings, and company info pages on Russian-language business development sites.

FIN7's decision to hire unwitting accomplices, as opposed to finding willing accomplices on the dark web, is likely due to greed. With willing accomplices, FIN7 would be forced to share a percentage of ransom payments totaling millions of dollars, whereas unwitting "employees" would work for monthly salaries in the low thousands, which are commensurate with the labor markets in post-Soviet states. However, FIN7's greed also afforded Gemini a view into the proprietary tools of this prolific threat team, as well as the exposure of another fake FIN7 company.

Correction (11/05/2021): The report incorrectly stated that a FIN7 system administrator was arrested in 2021. The individual was arrested in 2018 and sentenced in 2021. Four FIN7 members were arrested between 2018 and 2020.

Gemini Advisory Mission Statement

Gemini Advisory provides actionable fraud intelligence to the largest financial organizations in an effort to mitigate ever-growing cyber risks. Our proprietary software utilizes asymmetrical solutions in order to help identify and isolate assets targeted by fraudsters and online criminals in real-time.