MANDIANT

FIN11: A Widespread Ransomware and Extortion Operation

Table of Contents

FIN11: Widespread Email Campaigns as Precursor for Ransomware and Data Theft

- FIN11 is a well-established financial crime group that has recently focused its operations on ransomware and extortion.
- Their shift is emblematic of the changing nature of cyber criminal activity, which has become increasingly aggressive and difficult to ignore.
- Intrusive ransomware operations have sharply climbed in popularity with cyber criminals such as FIN11, supplanting other monetization schemes such as point-of-sale malware compromise.
- FIN11's brazenness was evident when they targeted pharmaceutical companies in early 2020, a time during which these organizations were especially vulnerable.

Overview

FIN11, a financially motivated threat group, has conducted some of the largest and longest running malware distribution campaigns Mandiant researchers have observed among financially motivated threat actors to date. In addition to high-volume malicious email campaigns, FIN11 is also notable due to their consistently evolving malware delivery tactics and techniques. Mandiant consultants have responded to multiple incidents where FIN11 has been observed monetizing their access to organizations' networks. Recent FIN11 intrusions have most commonly led to data theft, extortion and the disruption of victim networks via the distribution of CLOP ransomware. In at least one case, FIN11 previously deployed point-of-sale (POS) malware to at least one victim environment, suggesting a flexible and evolving approach to their intrusion operations.

Mandiant analysts primarily define FIN11 by campaigns observed since 2016 that use code families believed to be exclusive to the group (FlawedAmmyy, FRIENDSPEAK, MIXLABEL) as well as other overlapping tactics and techniques. There are notable overlaps between FIN11 and an activity set that security researchers call TA505. This term has been widely used in the security community to discuss large-scale spam campaigns which date to 2014 and have distributed various families including Dridex and multiple types of ransomware. FIN11 includes a subset of the activity publicly tracked as TA505, as well as an evolving arsenal of post-compromise tactics, techniques and procedures (TTPs) that have not been publicly reported on TA505. Notably, we have not attributed TA505's early operations to FIN11 and caution against conflation of the two clusters.

Targeting

FIN11 campaigns have impacted a wide variety of sectors and geographical regions. The group's malicious email campaigns from 2017 to 2018 primarily targeted organizations in the financial, retail and restaurant sectors. In 2019 and 2020, FIN11 expanded their targeting to a larger, more indiscriminate and diverse set of industries and countries, often using generic financial lures. However, a portion of FIN11's 2019 and 2020 campaigns targeted organizations in specific industries or regions, often using the target's native language coupled with manipulated email sender information, such as spoofed email display names and email sender addresses, to appear more legitimate. The shift in targeting observed during the past two years may be the result of FIN11's transition to ransomware as their main monetization method.

While organizations based in North America are most commonly cited as being impacted by well-known ransomware threats, alleged victims appearing on the CL0P^_-LEAKS website have most frequently been based in Europe; about half of the victim organizations have been based in Germany. While this data is skewed towards those who chose not to acquiesce to extortion demands, FIN11 has used German-language lures in many of their 2020 campaigns, suggesting that they have actively targeted German organizations.

Figure 1.

Victims appearing on CL0P^_-LEAKS website.

High-Volume and High-Tempo Campaigns

FIN11's consistent use of high-volume email distribution campaigns distinguishes the threat group from our other tracked FIN groups. When active, the actors have maintained a high operational tempo throughout 2019 and 2020, generally conducting multiple campaigns a week. Despite these high levels of activity, we have observed periods of varying lengths where FIN11 has seemingly taken breaks from conducting their email distribution campaigns. Most notably, FIN11 appears to have ceased operations completely from mid-March 2020 through late May 2020. While the length of this period of inactivity was atypical for FIN11, there are several possible explanations, including exercising caution following the FSB's arrests of more than 30 individuals in March 2020, a planned hiatus (such as holidays or exams), or a shift to focus on post-compromise activity or retooling.

While we have seen FIN11 email campaigns primarily use generic lures such as: "sales order," "bank statement," and "invoice," some of their campaigns have been tailored to the country or industry being targeted. For example, in January 2020, FIN11 initiated a series of malicious email distribution campaigns with email subjects such as "research report N-<five-digit number>" and "laboratory accident." Another operation in March 2020 used the lure "<pharmaceutical company name> 2020 YTD billing spreadsheet." Based on our visibility, these emails were sent primarily to pharmaceutical companies.

Table 1. Examples of language based and regional targeting.

Likely Organizational Targets	Lure Examples	Date
Spanish-language	LISTA DE PRECIO IFF.JULIO 2020 Factura Electronica	July 2020
Indian lanuages	<Indian Financial Institution> E NET6	June 2020
German-language	Angebot Tagesprotokoll 20.01.2020 Krankmeldung	September 2020
Korean-language	송금증 $<amount> 국세청송장 과세 요청	June 2019

Evolving Campaign TTPs

A hallmark of FIN11 activity since at least January 2019 has been the rapid evolution of their malicious email delivery TTPs. Throughout their 2019 and 2020 campaigns, the group has made small changes to their initial delivery mechanisms, likely in attempts to circumvent victims' detection regimes. These changes included the payload delivery methods, alterations to the downloaders in the macro-enabled documents, which Windows API functions were used by the FRIENDSPEAK downloader, lure languages and the payloads themselves. These relatively minor and less novel modifications, however, are not reflective of the group's sophistication.

From September 2019 through September 2020, FIN11 made incremental changes to the techniques used to deliver malicious Microsoft Office files containing FRIENDSPEAK payloads including the use of URL shortening services, HTML attachments, and compromised infrastructure. The group incorporated additional delivery techniques almost on a monthly basis, while also continuing to use techniques from prior campaigns. The timeline below illustrates the introduction of these TTPs from September 2019 through June 2020. FIN11 continued to modify their delivery tactics during Q3 2020; however, the changes were relatively minor. For example, in September 2020 the group implemented new evasion techniques to selectively choose which victims were redirected to domains that delivered malicious Office files. The timeline focuses on the delivery chain between the group's emails and associated malicious Office documents. The Office files almost always used macros to deliver the MINEDOOR dropper and the FRIENDSPEAK downloader. FRIENDSPEAK seemed to consistently deliver the MIXLABEL backdoor, (sometimes with a legitimate PuTTY Secure File Transfer Protocol (PSFTP) binary) but we did not always observe the secondary payload.

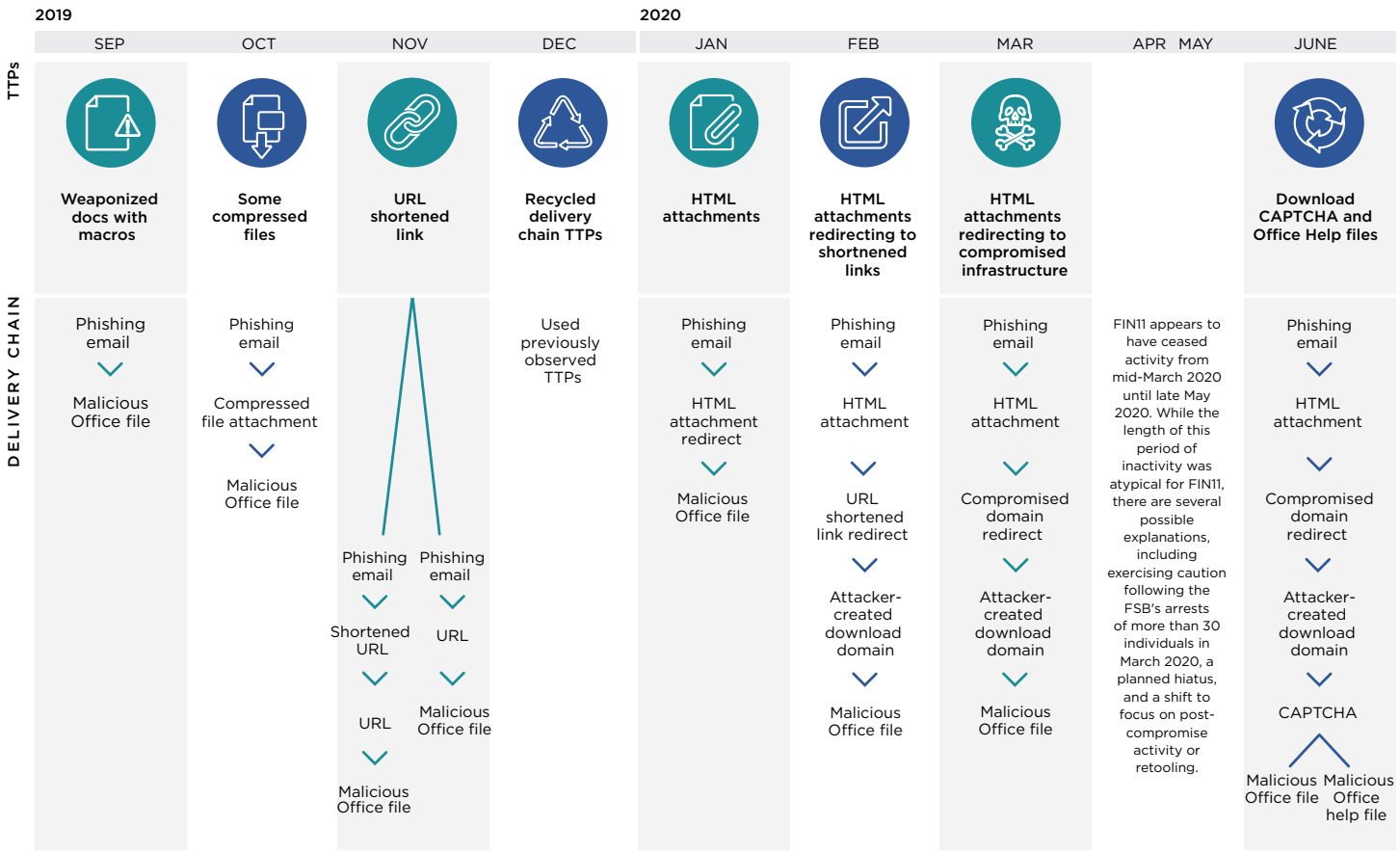


Figure 2.
FIN11 delivery TTPs across September 2019–June 2020 MINEDOOR and FRIENDSPEAK campaigns.

Hybrid Extortion

Despite the group's widespread high-volume email campaigns, we have only observed evidence of FIN11 successfully monetizing their operations in a handful of cases. In late 2018, Mandiant analysts observed FIN11 attempt to monetize their operations using the point-of-sale (POS) memory scraping tool BLUESTEAL. Since then, FIN11 has deployed CLOP ransomware at a variety of organizations. We observed the following TTPs during FIN11's CLOP deployments:

- Within a few days of the initial intrusion, FIN11 installed multiple backdoors, attempted to obtain domain administrator privileges and moved laterally within the impacted organization's network. While the backdoors used as initial footholds—FlawedAmmyy and MIXLABEL—may be exclusive to FIN11, the actors generally used common, publicly available tools during this phase.
- Prior to CLOP deployment, the actors used SALTLICK to disable Windows defender.
- The actors then used the NAILGUN installation and deployment tool to deploy CLOP, sometimes targeting hundreds of systems. Less frequently, the actors deployed CLOP with Group Policy Objects.
- FIN11 has often been quick to re-compromise hosts at organizations after losing access. For example, one organization was compromised via multiple FIN11 email campaigns within a matter of months. At another organization, several servers were infected with CLOP, restored from backups, and later re-infected.
- Victims of the CLOP ransomware were instructed to contact email addresses specified in ransomware notes, instead of being directed to a payment portal like some other ransomware operations. The ransom notes do not specify the ransom demand.

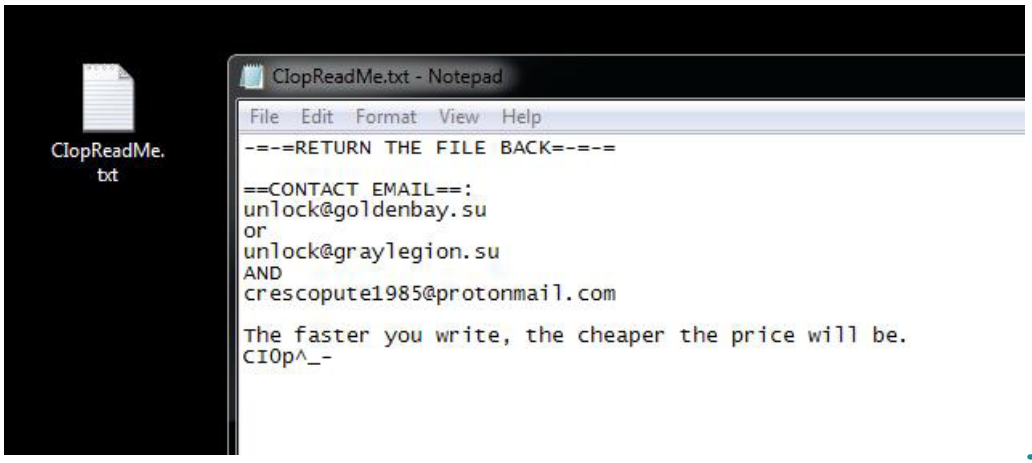


Figure 3.
CLOP ransom note example.

More recently, in 2020, FIN11 has evolved to conduct hybrid extortion attacks, combining ransomware with data theft to pressure their victims into acquiescing to extortion demands. In these cases, the actors accessed several dozen systems, staged data in RAR archives, uploaded the files to MegaSync servers, deployed CLOP ransomware and then sent an email threatening to publish the data. The exfiltrated data was later posted to a dark website named CL0P^_- LEAKS.

- In some instances, data was published in parts, probably to encourage victims to pay the ransom before more potentially damaging data was leaked.
- Mandiant consultants did respond to an intrusion in which FIN11 did not deploy CLOP ransomware but appeared to rely solely on data theft extortion. It is unclear if the actors had planned to eventually deploy CLOP.
- The actors have also used the website to advertise cyber security services, seemingly penetration testing, for $250,000 in Bitcoin.

Public reporting and data shared by the ransomware remediation firm Coveware suggests that FIN11 has demanded a wide range of ransom payments, ranging from a few hundred thousand dollars up to 10 million dollars. Notably, these extortion demands have seemingly increased since late 2019, which is likely a result of public reporting on companies' willingness to pay large ransoms as well as the introduction of hybrid extortion.

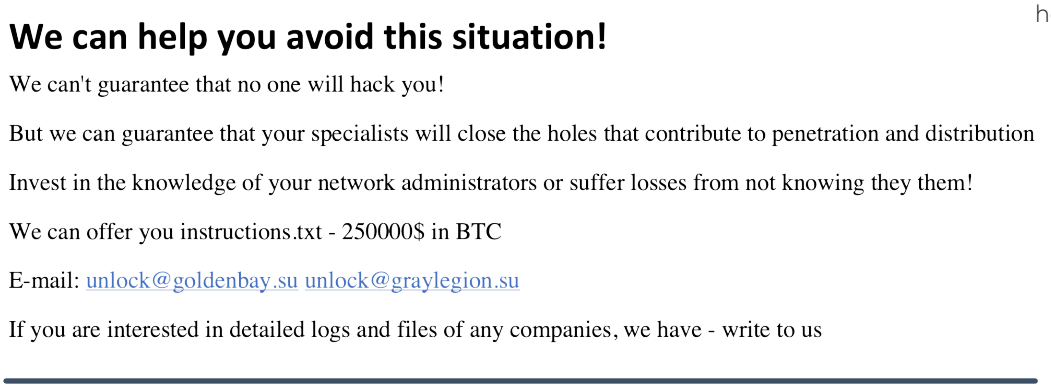


Figure 4.
Text from the CL0P^_- LEAKS home page.

Criminal Providers Enable FIN11 Operations

FIN11 has seemingly leveraged multiple criminal providers to conduct their operations. Their use of criminal providers is largely consistent with other financially motivated threat groups. Criminal actors can purchase a wide range of services and tools in underground communities—including private or semi- private malware capabilities, bulletproof hosting providers, various DNS-related services (including registration and fast-flux or dynamic DNS offerings) and code signing certificates—from actors who specialize in a single phase of the attack lifecycle. The outsourcing of tools and services associated with various parts of the attack lifecycle through criminal service providers can frustrate attribution efforts. Analysts may accidentally conflate activity between service providers and customers and imply a link between disparate groups based on indicators and TTPs that are attributable to a common service provider.

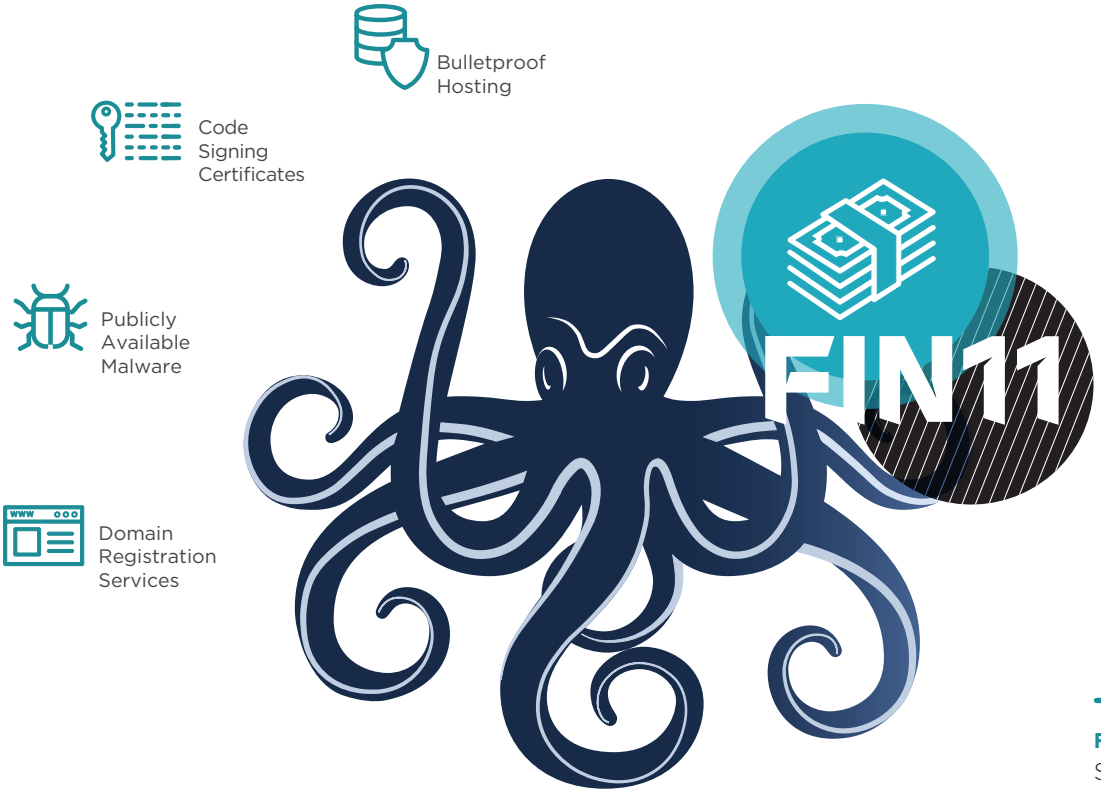


Figure 5.
Services used by FIN11.

Example 1: Possible Shared Droppers
Since fall 2019, FIN11 has used FORKBEARD, SPOONBEARD, and MINEDOOR to drop a variety of payloads. Public reporting does not distinguish between these droppers as they are quite similar and could be variants of the same malware family. In fact, there is at least one publicly available unpacker that works well across all variations we've observed. Comparison of representative samples from each of these variants identified a great deal of overlap with some key differences.

- The execution flow followed a very similar pattern of decoding and executing shellcode that would in turn decode and execute an embedded binary across all variants.
- While the families used different decoding algorithms, the supporting operations were very similar, including the use of similar arguments and variables used to index specific distances into arrays holding encoded data.
- Distinguishing features between each variation included minor changes to specific encoding algorithms, the storage and handling of XOR keys supporting those algorithms, and the inclusion of additional functions in otherwise extremely similar shellcode.

Based on the identified similarities, we suspect that a common builder with varying options, settings or polymorphic capabilities was used to create these droppers. However, we chose to track these variations separately because there are differences, although minor, in their encoding mechanisms, and there appear to be patterns in when or how they have been used.

- The MINEDOOR variant has dropped the FRIENDSPEAK downloader, and in a small number of instances, FlawedAmmyy.
- The FORKBEARD variant has almost exclusively been used to drop BARBWIRE, but we have also observed it dropping FlawedAmmyy.
- The SPOONBEARD variant has been used to drop a wide variety of FIN11 payloads, such as AndroMut, BARBWIRE, CLOP, EMASTEAL, FlawedAmmyy, FLOWERPIPE, and SALTLICK.

It is possible that these droppers, or the builder used to create them, are not exclusive to FIN11 based on several instances in which they have dropped malware typically associated with other threat groups. This could indicate that either a builder used to generate the droppers is offered on underground forums or FIN11 has overlapping membership with other threat groups.

Table 2. Droppers employed by FIN11 and associated payloads.

Dropper	Dropped Families	Examples
SPOONBEARD	Amadey AndroMut AZORult BARBWIRE CLOP EMASTEAL FlawedAmmyy FLOWERPIPE JESTBOT POPFLASH SALTLICK SCRAPMINT SLOWROLL TINYMET VIDAR	In May 2019, a SPOONBEARD-packed SCRAPMINT sample was uploaded to VirusTotal. Based on several Mandiant incident response cases, we believe SCRAPMINT has been used by multiple actors to conduct POS malware operations including FIN6. Between August and December 2019, we identified SPOONBEARD samples that delivered AZORult or VIDAR credential theft malware. It is plausible that FIN11 used these credential stealers; however, both AZORult and VIDAR have been sold on underground forums and are used by multiple actors. In late 2019 and early 2020, we identified SPOONBEARD samples that delivered SLOWROLL and JESTBOT respectively. SLOWROLL is a backdoor associated with TEMP.TruthTeller (aka Silent Group) post-compromise activity.
FORKBEARD	BARBWIRE FlawedAmmyy SHORTBENCH Meterpreter	We observed FORKBEARD dropping SHORTBENCH and Meterpreter in an April 2020 intrusion. FIN11 has used these Metasploit-related tools; however, we currently have inadequate evidence to attribute this intrusion to FIN11. SHORTBENCH and Meterpreter are used by a variety of actors.
MINEDOOR	FlawedAmmyy FRIENDSPEAK MINEBRIDGE	In January 2020, Mandiant experts identified email campaigns that used MINEDOOR to deliver the MINEBRIDGE backdoor. The limited overlap in TTPs between these campaigns and contemporaneous FIN11 campaigns may suggest MINEDOOR is not exclusive to FIN11.

Example 2: Possible Use of Code Signing Service

Throughout 2019 and to a lesser extent in 2020, FIN11 used valid code signing certificates to sign their malware, likely to increase the effectiveness of their campaigns. Sensitive sources indicate that at least one actor who advertises code signing certificates on underground forums likely sold a certificate using a name that overlapped with a certificate used to sign FIN11 attributed samples. Many of these certificates share common characteristics, such as the use of UK-based organizations with incorrect physical addresses as the certificate's subject. While looking for certificate overlaps across samples, we identified many instances where seemingly unrelated malware was signed with certificates that shared a common subject. The use of code signing certificates with overlapping characteristics by what appears to be multiple unrelated threat actors seems an unlikely coincidence and suggests that these certificates are being acquired from a common source.

- Multiple certificates were associated with the same organization and were often issued by the same certificate authority. The organizations largely appeared to be small businesses. In addition, the certificates containing the names of these organizations did not list accurate physical addresses.
- As one example, we identified at least eight distinct certificates that share the common name value "ET HOMES LTD". We have not attributed all of the samples using these certificates to FIN11. Other samples signed by certificates sharing the same common name value included AZORult, GANDCRAB, GODZILLA LOADER, and BETABOT.

Table 3. ET HOMES LTD common name certificate overlap.

MD5	Malware Families	Issuing CA	Public Key MD5
c94f47e8f25c3b41df97ecb3c23ccf5d	FlawedAmmyy, MINEDOOR	Thawte	24016bd5a1e0c03474cb97c1253a5dad
a19ebe61347b91f997257cf3104b9621	AZORult, Godzilla, Remcos	Comodo	dfd53dd143e1d904d16fae05e929a8f9
87cf140238fd26a03b815bb229eef009	GANDCRAB	Comodo	89c9a36bb642b0b8dfb0cdc6ae9e5238
b7dfc43bdd46c560a3e32d6aea25bc8a	AZORult, GANDCRAB, GODZILLA	Comodo	ce2b80abfbc72c0a74d3745ca3faedfe
491ef81a6f6f1849797b39091a6046de	AZORult	Comodo	024e15a4287dad10a8314d8c2c593651
6d3b27150b04d94ffa77441132f8f24a	AZORult	Comodo	c8439866c526ccd673f2aeed0be2f894
d2c06720c0896a50ecaa5a27633be1d3	AZORult	Comodo	10a54f36e3a95e802f5ff5a2773110c8
169b1841347ebb2d43a326417a6f05bd	AZORult, BETABOT	Comodo	7324e4ed9fbc1d1b157e8433fc30740b

Potential Commonwealth of Independent States Origin

We assess with moderate confidence that FIN11 is likely operating out of the Commonwealth of Independent States (CIS) based on Russian-language file metadata, avoidance of CLOP deployments in CIS countries, and the observance of the Russian New Year and Orthodox Christmas holiday period.

- A number of FIN11's files contain metadata that suggest the operators are using a language with a Cyrillic alphabet.
- Samples of CLOP ransomware check for keyboard layouts commonly used in the CIS countries and for the Russian character set (204) before execution. If both the keyboard layout and character suggest the host is in a CIS country, CLOP will delete itself.
- FIN11's activity appears to drop off dramatically during the Russian New Year holiday and Orthodox Christmas, which occurs between January 1–8 each year.

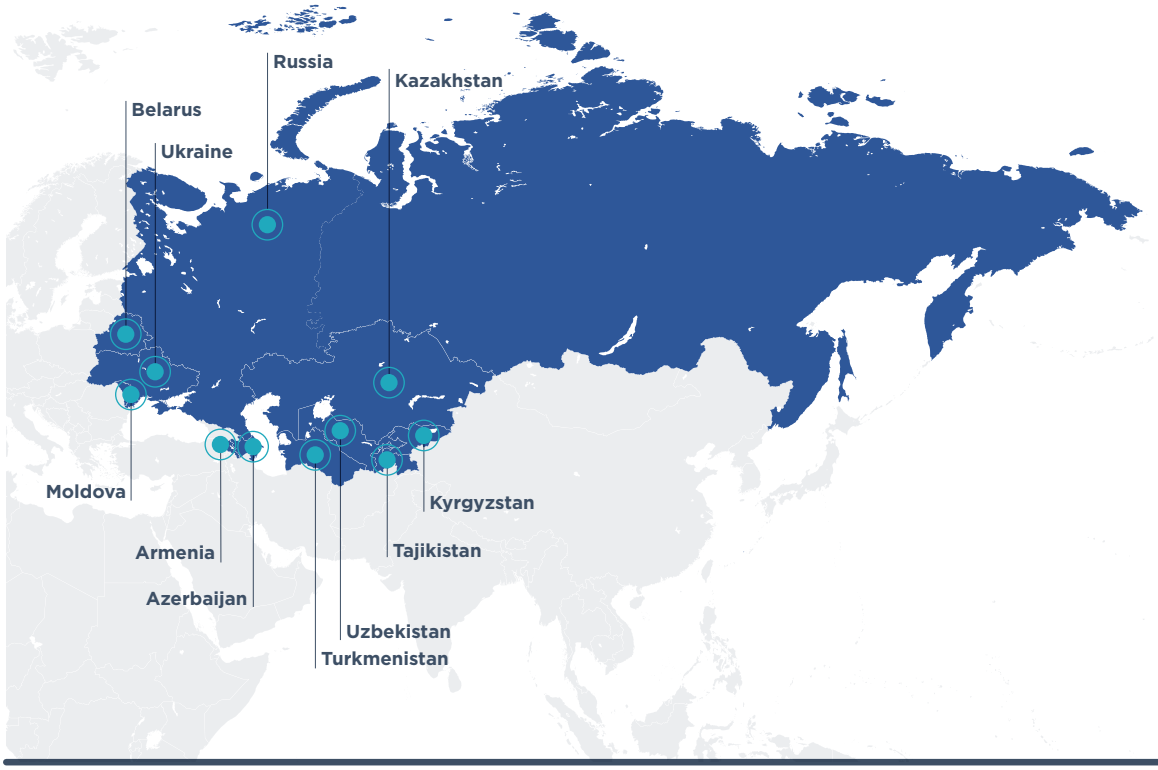
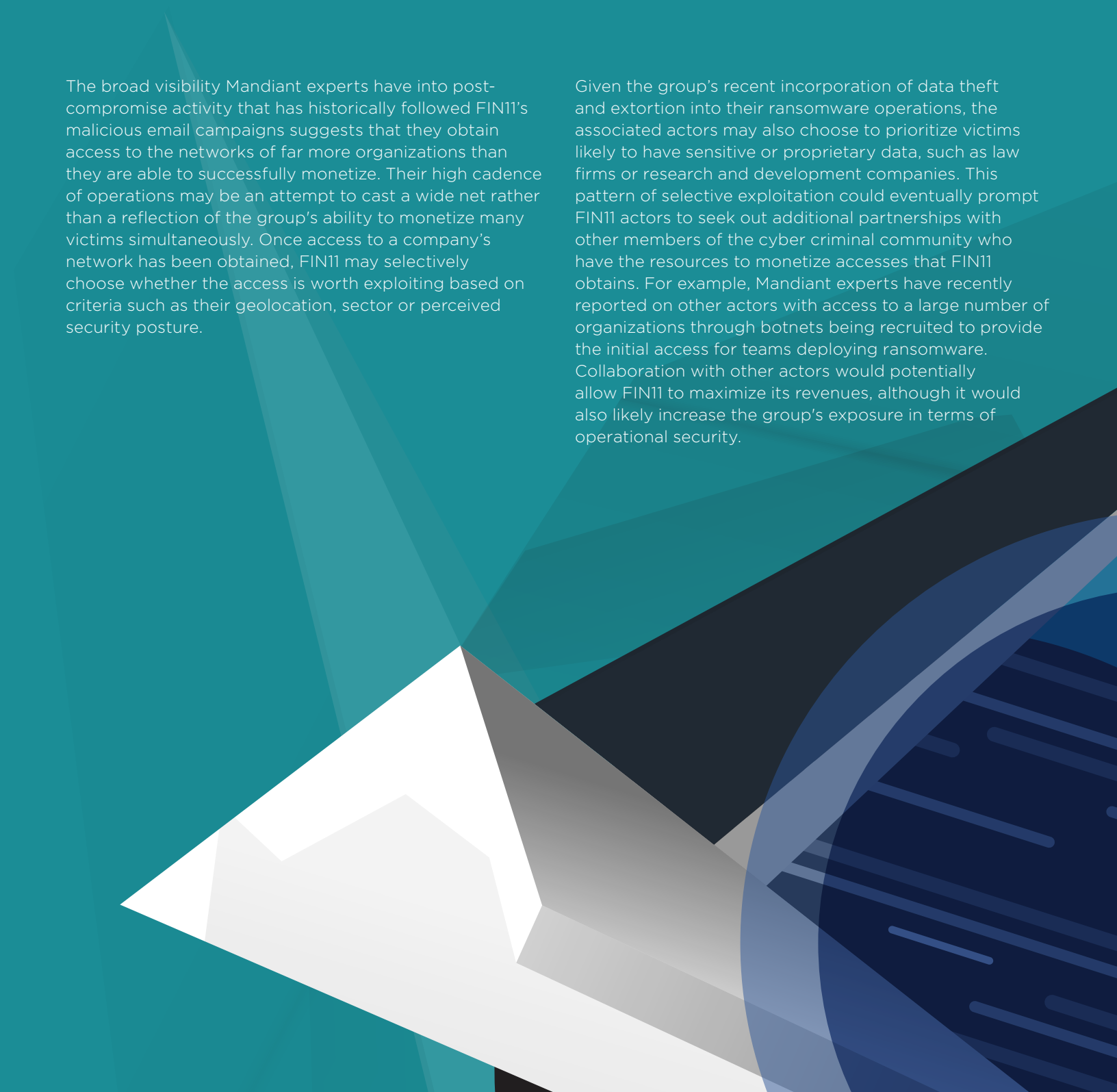


Figure 6. Founding and member Commonwealth of Independent States (CIS) nations.

Outlook and Implications

The broad visibility Mandiant experts have into post-compromise activity that has historically followed FIN11's malicious email campaigns suggests that they obtain access to the networks of far more organizations than they are able to successfully monetize. Their high cadence of operations may be an attempt to cast a wide net rather than a reflection of the group's ability to monetize many victims simultaneously. Once access to a company's network has been obtained, FIN11 may selectively choose whether the access is worth exploiting based on criteria such as their geolocation, sector or perceived security posture.

Given the group's recent incorporation of data theft and extortion into their ransomware operations, the associated actors may also choose to prioritize victims likely to have sensitive or proprietary data, such as law firms or research and development companies. This pattern of selective exploitation could eventually prompt FIN11 actors to seek out additional partnerships with other members of the cyber criminal community who have the resources to monetize accesses that FIN11 obtains. For example, Mandiant experts have recently reported on other actors with access to a large number of organizations through botnets being recruited to provide the initial access for teams deploying ransomware. Collaboration with other actors would potentially allow FIN11 to maximize its revenues, although it would also likely increase the group's exposure in terms of operational security.



To learn more about Mandiant Solutions, visit: **www FireEye.com/mandiant**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

M-EXT-SR-US-EN-000324-01

About Mandiant Solutions
Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

MANDIANT®