FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets

mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets

Today, Mandiant Intelligence is releasing a comprehensive report detailing FIN12, an aggressive, financially motivated threat actor behind prolific ransomware attacks since at least October 2018. FIN12 is unique among many tracked ransomware-focused actors today because they do not typically engage in multi-faceted extortion and have disproportionately impacted the healthcare sector. They are also the first FIN actor that we are promoting who specializes in a specific phase of the attack lifecycle—ransomware deployment—while relying on other threat actors for gaining initial access to victims. This specialization reflects the current ransomware ecosystem, which is comprised of various loosely affiliated actors partnering together, but not exclusively with one another.

The full published report covers historical and ongoing activity attributed to FIN12, their use of partners to enable their operations, including initial access providers, the evolution of the group’s tactics, techniques, and procedures, and trends in their extensive use of Cobalt

Strike BEACON.

The Mandiant Security Validation (Validation) Behavior Research Team (BRT) has created VHR20210922 – FIN12, which is accessible on the Content page of the Validation Customer Portal.

We are also releasing the following reports referenced in the report to Mandiant Advantage Free.

- Multiple Threat Actors Deploy RYUK Using Varying TTPs
- Ryuk Malware Profile
- Analysis of Loader and Backdoor Combinations Associated with TRICKBOT Operators Used to Enable Post-Intrusion Ransomware Deployment

Figure 1: FIN12 badge

FIN12 Victims

FIN12's operations provide illustration that no target is off limits when it comes to ransomware attacks, including those that provide critical care functions. Almost 20 percent of directly observed FIN12 victims were in the healthcare industry and many of these organizations operate medical facilities. We observed FIN12 activity at healthcare organizations both before and after the joint alert by multiple U.S. government entities in October 2020 that warned of an "increased and imminent" threat to hospitals and medical facilities. This targeting pattern deviates from some other ransomware threat actors who had at least stated an intention to show restraint in targeting hospitals, especially throughout the

COVID-19 pandemic. FIN12’s remaining victims have operated in a broad range of sectors, including but not limited to business services, education, finance, government, manufacturing, retail, and technology.

While these victim organizations have been overwhelmingly located in North America, there is some evidence that FIN12's regional targeting is expanding. Nearly 85 percent of the group’s known victims have been based in North America, however, we observed twice as many victim organizations based outside of North America in the first half of 2021 than we observed in 2019 and 2020 combined. Collectively, these organizations have been based in Australia, Colombia, France, Indonesia, Ireland, the Philippines, South Korea, Spain, the United Arab Emirates, and the United Kingdom. This shift could be due to various factors such as FIN12 working with more diverse partners to obtain initial access and increasingly elevated and unwanted attention from the U.S. government.

We believe that the most significant factor in FIN12’s targeting calculus has been a victim’s annual revenue. The vast majority of known FIN12 victims have more than $300 million USD in revenue, based on corporate financial data compiled from ZoomInfo. While this data is skewed to our direct visibility, FIN12 does appear to consistently target larger companies in comparison to the average ransomware affiliate. Targeting victims that meet a certain revenue threshold also aligns with underground forum activity; some threat actors, including those using RYUK, have specified different ranges of minimum requirements for potential victims’ annual revenue. Further, comments detailing revenue information in malware administration panels operated by FIN12’s initial access providers illustrate that this is a relevant factor for victim selection or at minimum for prioritization of available targets. FIN12’s selection of high-value targets is consistent with the broader trend of threat actors pursuing larger targets in recent years, almost certainly because of the perception that it justifies proportionally large ransom demands.

Parasites And Symbiotes

From the beginning of their operations and until March 2020, we observed FIN12 exclusively leverage TRICKBOT accesses as a launching point for their ransomware attacks. However, after returning from a nearly four-month hiatus in August 2020, the initial access vectors leveraged by FIN12 became increasingly diversified. In at least some cases, these variations may reflect the use of distinct initial access providers. For example, beginning in early 2021, we directly observed several cases where the first evidence of FIN12 activity was a login to a victim’s Citrix environment. This activity is also consistent with our identification of multiple Russian-speaking actors operating in underground communities seeking partners who could provide Citrix accesses for RYUK ransomware operations. Although we currently lack sufficient evidence to attribute these actors to FIN12, these solicitations nonetheless further support the likelihood that FIN12 has not relied on a single initial access provider to enable their operations. This division of labor is not uncommon and reflects the professionalism and specialization of the cybercrime ecosystem overall.

In many incidents, where the initial intrusion vector was identified, FIN12 activity was observed on the same day as the initial access campaign suggesting that FIN12 maintains a close relationship with at least some threat actors providing them access. Most notably, FIN12 maintains a close relationship with TRICKBOT and BAZARLOADER affiliated actors. Beyond leveraging accesses obtained via these families, FIN12 has used overlapping toolsets and services including backdoors, droppers, and codesigning certificates. Despite these similarities, we track FIN12 as a distinct threat actor given their specific role in the deployment of ransomware, their ability to work independently of these families, and our observations of other distinct threat actors who also deploy ransomware using accesses obtained via these malware ecosystems.

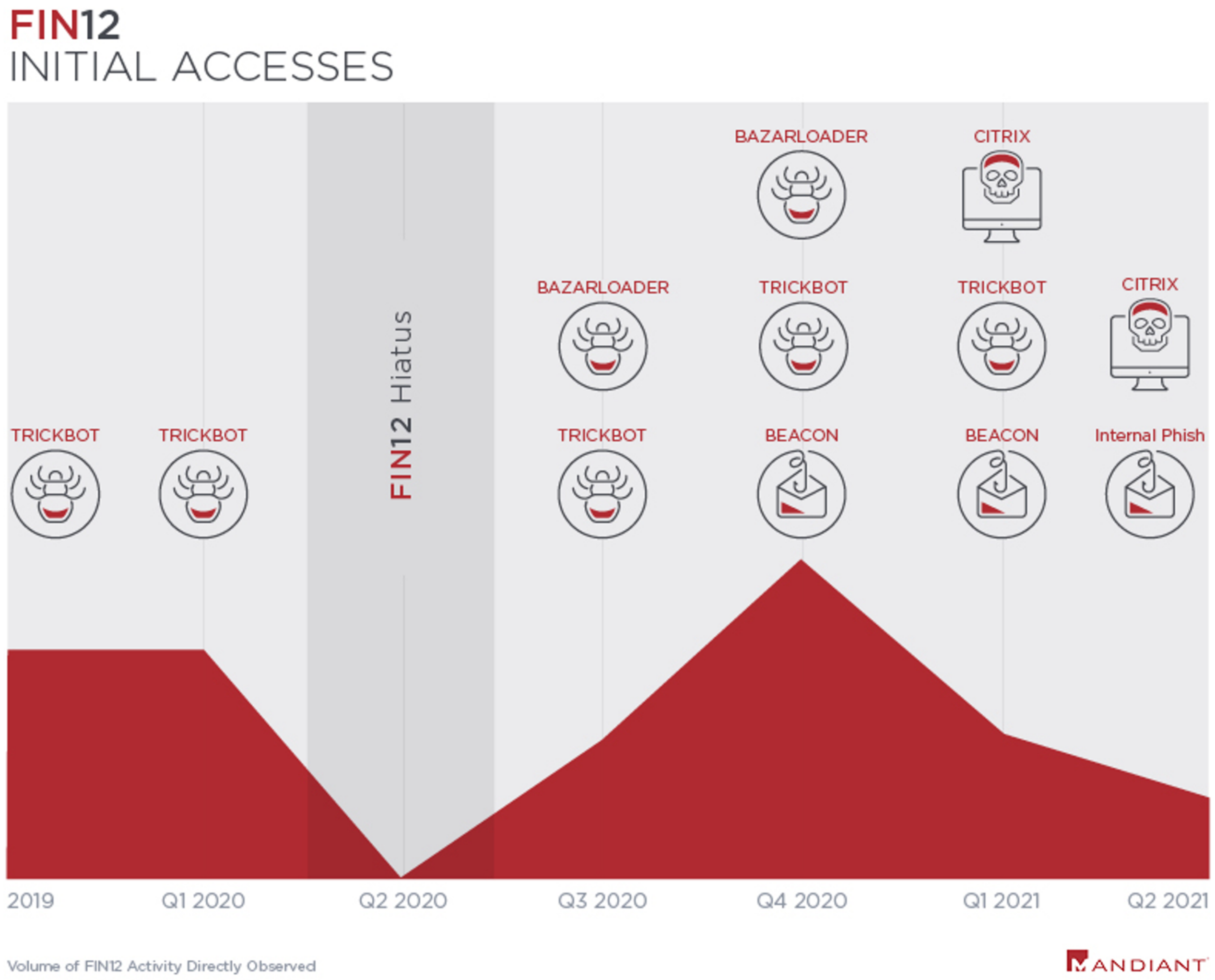

Figure 2: Directly observed initial accesses leveraged by FIN12

Prioritizing Speed

FIN12's reliance on other threat actors to obtain initial access to organizations and their specific focus on ransomware deployment has paid dividends in terms of their time-to-ransom (TTR). We calculate the TTR as the amount of time from when they first access an environment to when they begin to deploy ransomware. In the first half of 2021, as compared to 2020, FIN12 significantly improved their TTR, cutting it in half to just 2.5 days. These efficiency gains are enabled by their specialization in a single phase of the attack lifecycle, which allows threat actors to develop expertise more quickly. FIN12 also stands out in the pack of ransomware operators today because they do not usually engage in multifaceted extortion—a tactic that has become commonplace in today's threat landscape. The most significant factor in FIN12's decision to refrain from stealing victim data and publicly shaming victims may be the impact it has on the speed of their operations. The average TTR across our FIN12 engagements involving data theft was just under 12.5 days compared to 2.5 days where data theft was not observed. Each additional day FIN12 spends in an environment before completing their objective increases their risk being detected. FIN12's apparent success without the need to incorporate additional extortion methods likely suggests the notion that they to not believe spending additional time to steal data is worth the risk of having their plans to deploy ransomware thwarted.

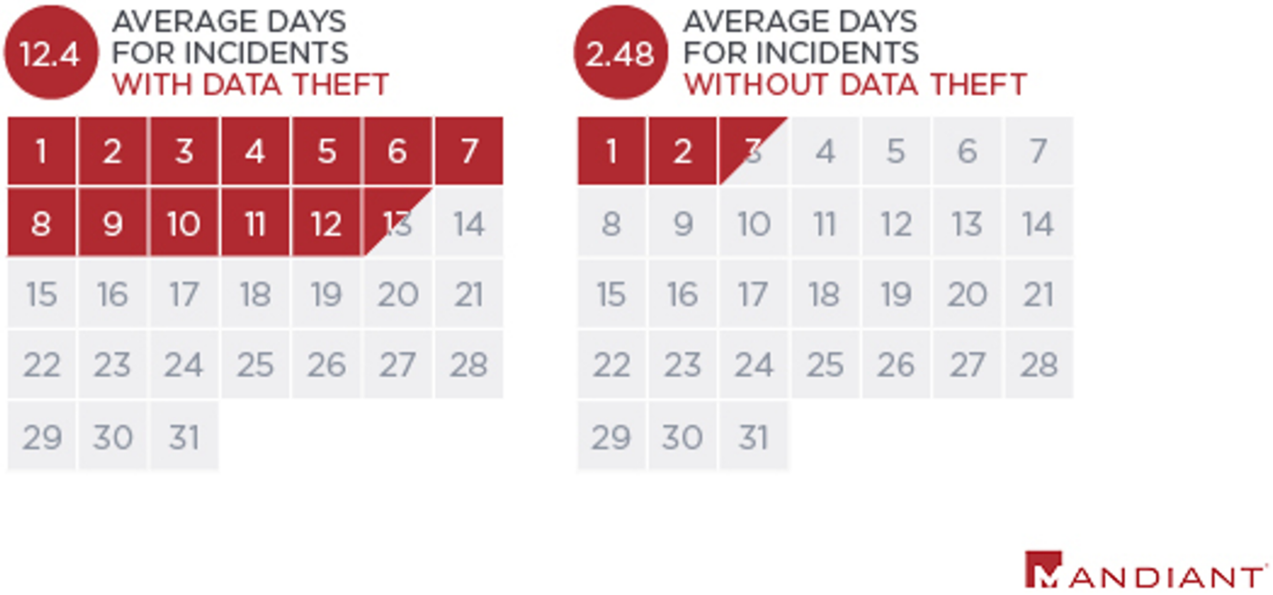

Figure 3: FIN12's Time-to-Ransom (TTR)

Implications

While threat actors running ransomware-as-a-service (RaaS) outfits have an important role in multifaceted extortion attacks, the focus on the branding and communication components of these services can detract from other important players. Intrusion actors, such as FIN12, may arguably play a more pivotal role in these operations, yet have received marginal attention. These actors are the ones navigating victim networks and deploying the ransomware itself, and in at least some cases, may have direct input into the target selection. The skillset required for this role may be comparatively less developed within the cyber-criminal underground, which has historically put a heavy emphasis on malware development, distribution, and the management of cash-out operations. We also constantly observe solicitations from threat actors looking to recruit individuals to join intrusion teams, sometimes even trying to hire individuals under false pretenses, facts that may be reflective of a talent shortage in this area. Notably, intrusion groups do not typically have an allegiance to any particular RaaS brand and have exhibited that they can easily switch between or use multiple brands concurrently. The shifting nature of these allegiances is a key reason for why intrusion operators such as FIN12 are important for security teams and organizations to understand and track rather than maintaining an exclusive focus on the brands and ransomware families these operators choose to distribute at a given moment.

Download FIN12 report today.

Acknowledgements

A small army contributed to the research, malware analysis, data analysis, writing and review of this report, and without them this could never have seen the light of day. We also owe an extreme debt of gratitude to the many thousands of hours of hard work put in by our incident responders, Managed Defense analysts, Advanced Practices teams, and underground researchers who collected and normalized much of the data that formed the basis for our analysis.Every report published by Mandiant is a massive team effort and we are grateful for the opportunity to work with a world class group of professionals in all their different areas of practice. Unfortunately, for the sake of brevity, we cannot list the name of every person who contributed to this work but we would like to specifically call out the efforts of a few individuals and teams.

The following people and teams provided critical analysis support to the team working on this report:

Jordan Nuce

Ioana Teaca

Van Ta

Aaron Stephens

Bryce Abdo

Sandor Nemes

Jessa Valdez

Thomas Pullen

Moritz Raabe

Amsterdam and Ukraine research offices

Finally, extra special thanks to Ana Foreman for putting together the graphics that went into this reporting, and her infinite patience with our many edits.

Mandiant Security Validation Actions

Organizations can validate their security controls using the following Actions with Mandiant Security Validation.

Network Actions

VID	Title
A100-040	Malicious File Transfer - RYUK, Download, Variant #2
A100-042	Malicious File Transfer - RYUK, Download, Variant #3
A100-044	Malicious File Transfer - RYUK, Download, Variant #4
A100-071	Malicious File Transfer - RUBEUS Tool, Download
A100-072	Malicious File Transfer - SYSTEMBC, Download
A101-850	Command and Control - GRIMAGENT, C2 Traffic, Variant #2
A101-851	Command and Control - GRIMAGENT, C2 Traffic, Variant #1
A101-852	Malicious File Transfer - GRIMAGENT, Download, Variant #1
A101-853	Command and Control - GRIMAGENT, C2 Traffic, Variant #4
A101-854	Command and Control - GRIMAGENT, C2 Traffic, Variant #3
A101-855	Malicious File Transfer - GRIMAGENT, Download, Variant #3
A101-856	Malicious File Transfer - GRIMAGENT, Download, Variant #2
A101-858	Malicious File Transfer - WEIRDLOOP, Download, Variant #2
A101-859	Malicious File Transfer - WEIRDLOOP, Download, Variant #1

A101-862	Malicious File Transfer - MALTSHAKE, Download, Variant #2
A101-863	Malicious File Transfer - MALTSHAKE, Download, Variant #1
A101-864	Malicious File Transfer - ICECANDLE, Download, Variant #3
A101-865	Malicious File Transfer - ICECANDLE, Download, Variant #2
A101-882	Malicious File Transfer - FIN12, Get-DataInfo.ps1, Download
A101-886	Malicious File Transfer - KERBRUTE, Download, Variant #2
A101-909	Lateral Movement - FIN12, RYUK, Execution with PsExec
A101-910	Lateral Movement - FIN12, RYUK, Transfer with PsExec
A101-911	Phishing Email - Malicious Attachment, FIN12, WEIRDLOOP
A101-912	Malicious File Transfer - FIN12, ADFIND Batch Script
A101-920	Phishing Email - Malicious Attachment, FIN12, BAZARLOADER
A101-921	Malicious File Transfer - BAZARBACKDOOR, Download
A101-922	Command and Control - FIN12, BEACON, Check-In
A101-923	Command and Control - FIN12, DNS Query, Variant #1
A101-924	Command and Control - FIN12, DNS Query, Variant #2
A101-925	Command and Control - FIN12, DNS Query, Variant #3
A101-926	Command and Control - FIN12, DNS Query, Variant #4
A101-927	Command and Control - FIN12, DNS Query, Variant #5

Endpoint Actions

VID	Title
A104-003	Host CLI - RYUK, FIN12, Active Directory Reconnaissance
A104-004	Host CLI - Scheduled Task Called by Run Key, Default Privileges
A104-007	Host CLI - Scheduled Task Called by Run Key, Highest Privileges
A104-012	Protected Theater - RYUK Actor Modify File Permissions
A104-710	Protected Theater - RYUK Actor, Kill Services and Processes
A104-831	Protected Theater - GRIMAGENT, Schtask and Registry for Persistence
A104-842	Protected Theater - FIN12, RYUK, Download and Execution via BITSAdmin
A104-856	Host CLI - FIN12, Active Directory Reconnaissance