proofpoint.

REPORT

Threat Update

Premium Threat Information Services

This document was provided to Threat Intelligence Services customers on 04 November 2021 and has been modified to exclude identifiable information and customizations. The information and recommendations in this document remain relevant to ongoing landscape activity. For more information, contact your account team.

Last Updated: 04 NOVEMBER 2021

Table of Contents

FIN12 – An Ecosystem Subsuming Multiple Proofpoint-Tracked Threat Actors

Mandiant-named FIN12[1], formerly known as UNC1878, is a financially motivated group with a close relationship to some of The Trick and BazaLoader affiliated actors. FIN12 relies on these affiliates to gain initial access to targeted environments; this access can then be used by FIN12 to deploy ransomware post-compromise. Although Proofpoint-tracked actors do not directly map one-to-one with this specific actor, we frequently observe these initial access payloads delivered via email. This Threat Update highlights the initial access actors tracked by Proofpoint, including TA547, TA551, and TA578, which likely share overlap with the initial access brokers used by FIN12.

KEY TAKEAWAYS

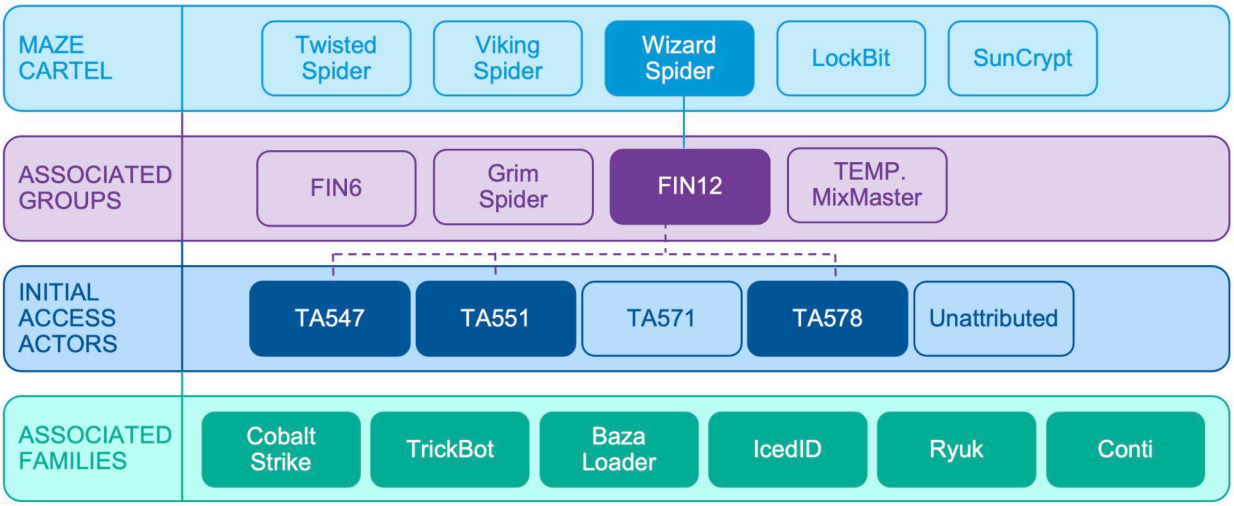
- FIN12 maintains a close relationship with The Trick- and BazaLoader-affiliated actors and uses these payloads to gain initial access into target networks to ultimately deploy Conti (formerly Ryuk) ransomware. Proofpoint frequently observes The Trick and BazaLoader as initial access payloads delivered via email.
- There are documented infection chains linking Conti deployment following initial compromise with BazaLoader and The Trick.
- Threat actors distributing The Trick and IcedID are connected by their use of shared group tags (gtags) and overlapping command and control (C2) infrastructures.
- In the days from 9 August to 31 October, the primary distributors of BazaLoader, The Trick, and IcedID have been TA547, TA551, and TA578.
- Based on Proofpoint-observed tactics, techniques, and procedures (TTPs) and open-source reporting, it is likely that TA547, TA551, and TA578 are likely paid Initial Access Brokers (IABs) for FIN12.

FINDINGS

Background

Wizard Spider[2] is a suspected member of the Maze Cartel, which is one of the world's first cyber-cartels and the developer of The Trick, Ryuk, Conti, and other tools. This group does not openly advertise on the darknet, "indicating that WIZARD SPIDER likely only sells access to, or works alongside, trusted criminal groups."[3] These trusted criminal groups are paid a wage[4] rather than a percentage of the proceeds from a successful attack. Wizard Spider continues to actively deploy Conti ransomware and update the Conti data leak site.[5]

[1] https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets
[2] https://attack.mitre.org/groups/G0102/
[3] https://adversary.crowdstrike.com/en-US/adversary/wizard-spider/
[4] https://media.defense.gov/2021/Sep/22/2002859507/-1/-1/0/CSA_CONTI_RANSOMWARE_20210922.PDF
[6] https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/



FIN12 is well-known for their association with the group dubbed "Wizard Spider", as well as their rapid deployment of Ryuk and its successor,[6] Conti. The closely coupled nature of BazaLoader and The Trick as an initial access vector with Conti is well-established. Since at least 2018, FIN12 has used The Trick in the early phases of the attack lifecycle to gain initial access. FIN12 has also on occasion leveraged the same code-signed payloads used by BazaLoader affiliates. The group began deploying BazaLoader in Q3 2020, coinciding with an attempt by multiple cybersecurity vendors to take down[7] the backend infrastructure of The Trick botnet. Although the impact of the disruption was short-lived, FIN12 continued to diversify their initial access partnerships well into 2021. According to Mandiant, Cobalt Strike almost exclusively replaced Empire as FIN12's primary persistence tool in nearly every intrusion since February 2020.

Targeting

The members of the Maze Cartel, such as Wizard Spider, use big game hunting (BGH) tactics, targeting high-revenue victims for high-value payouts. There are minimum revenue requirements for targets, confirming financial motivation for these groups. In 2020, 85%[8] of FIN12's targets earned more than 300 million USD. Also in 2020, as many ransomware groups were declaring the healthcare sector "off-limits" due to the pandemic, Conti actors continued to attack the sector. In May 2021, the FBI identified[9] at least 16 Conti ransomware attacks that targeted U.S. healthcare over the last year. During that same time, nearly 20% of FIN12's targets were in the healthcare sector.

INITIAL ACCESS ACTORS

FIN12 works closely with The Trick and BazaLoader affiliated actors and "has likely established close partnerships with these initial access providers."[10] Proofpoint frequently observes BazaLoader, The Trick, and Cobalt Strike being distributed by unattributed actors as well. While that activity is outside the

[6] https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
[7] https://www.noticeofpleadings.com/trickbot/
[8] https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets
[9] https://s3.documentcloud.org/documents/20785651/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf
[10] https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets

scope of this report, the clustering of activity supports the theory that the larger IAB ecosystem continues to evolve and mature. The primary distributors and likely trusted deployers of BazaLoader, The Trick, and IcedID according to Proofpoint data in the last 90 days have been TA547, TA551, and TA578. The key differences between Proofpoint-tracked initial access brokers TA547, TA551, and TA578 and Mandiant's FIN12 actor is the deployment of ransomware; Proofpoint does not have visibility into the post-infection deployment of ransomware, whereas that is the key differentiator for Mandiant's FIN12. However, Proofpoint tracked actors are linked to FIN12 by payloads, timing, and overlapping services and infrastructure. While FIN12 can and has worked independently of initial access actors, their reliance on IABs allows them to specialize in ransomware deployment and play a more active role with "hands on keyboard" activity.

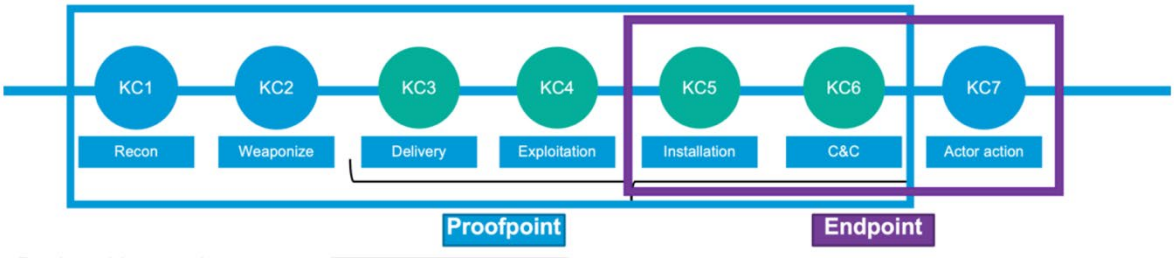


Figure 2: Proofpoint's visibility of the IAB infection chain

TA547

TA547 is a long-time distributor of The Trick and the most prolific IAB focused on this malware according to Proofpoint telemetry since Emotet's January 2021 takedown[11]. Proofpoint researchers suspect that this actor is a malware distribution service, providing initial access via The Trick and occasionally BazaLoader. FIN12 frequently uses The Trick to gain initial access and deploy secondary payloads. Researchers at Mandiant suspect that "in most or all cases these secondary payloads were deployed via TRICKBOT as a means of handoff between teams or individual operators and used by FIN12 to maintain a foothold in the environment while performing later-stage tasks."[12]

Proofpoint has observed that The Trick actors re-use C2 infrastructure throughout versions. For example, Proofpoint observed near complete re-use in C2 infrastructure for The Trick version 100019. This version has been used since early August 2021 and has been associated with gtags – unique affiliate identifiers for instances of the Trick – "Rob136" and "Soc1" (TA547), "Leg1" and "Sat4" (Unattributed), and others during that timeframe.

TA551

Proofpoint researchers suspect that, like TA547, TA551 is likely selling access for other actors. TA551 has cycled through several different malware payloads since 2019. This section highlights their delivery of The Trick, BazaLoader, and IcedID. According to Crowdstrike,[13] the crossover of "tin"/ "sin" gtags in IcedID and The Trick show a larger relationship between the IcedID groups and distributors of The Trick.

[11] Editor's note, 28 January 2022: Emotet has since returned to activity. While it does not appear to be distributing The Trick as a secondary payload at this time, many researchers have speculated about ongoing interactions between the groups, including shared infrastructure.
[12] https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets
[13] https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/

TA551 has been consistently distributing The Trick and BazaLoader since June 2021, almost exclusively delivering BazaLoader since September 2021. Since February 2019, TA551 has delivered The Trick with at least eight different gtags. Proofpoint observed a break of TA551 activity delivering The Trick from November 2019 through April 2021.

From August to October 2021, Proofpoint observed 46 TA551 campaigns; of those, 40 distributed BazaLoader, three distributed The Trick, but none contained IcedID. That is in stark contrast to their campaign activity from May to July 2021 when they distributed four BazaLoader campaigns, 17 The Trick campaigns and 24 IcedID campaigns.

TA578

FIN12 shifted from The Trick to BazaLoader late in September 2020. The Bazaloader payload is primarily distributed via malicious email campaigns and used to download BazaBackoor, which can be used to deliver Cobalt Strike Beacon. TA578 first appeared in Proofpoint data on 27 May 2020, around the same time Conti ransomware rebranded from Ryuk ransomware. This actor distributed various payloads, including Ursnif, IcedID, and Buer throughout summer 2020. When TA578 resurfaced in Proofpoint data in July 2021, they were distributing BazaLoader/BazaBackdoor using the same legal-themed "contact us" lure that appeared in their 2020 campaigns. BazaLoader soon became the preferred payload of TA578, appearing in 20 of their 23 campaigns from July 2021 to October 2021. The remaining three campaigns contained IcedID and/or Sliver.

Two separate DFIR reports on full kill chain Conti infections line up with TA578 campaigns observed at Proofpoint. The May 2021 report[14] described a threat actor going from IcedID to deploying Conti within 2.5 days. The September 2021 report[15] investigated a BazaLoader campaign that deployed Cobalt Strike and ended with Conti. In both reports, the campaigns began with a malicious email containing a zipped JavaScript attachment that, when executed, downloaded IcedID or BazaLoader. Based on timing, malware, C2, and message theme, it is likely that TA578 was the actor delivering both payloads.

RECOMMENDATIONS

Proofpoint recommends that, given the potential for delivery of a range of big game hunting ransomware associated with the various initial access payloads TA547, TA551, and TA578 distribute, organizations should aggressively investigate and remediate delivered threats from these groups.

- Implementation of defense-in-depth approaches to detection and mitigation of delivered payloads.
- Maintain URL rewriting best practices and minimize safelisting, especially for contact form submissions.
- Consider the use of browser isolation and enforce VPN usage for remote workers to ensure that layered protections can be maintained regardless of location.
- Ingest C2 for The Trick actors. The version patterns for The Trick show that C2 overlap occurs between separate versions and the actors re-use C2 for months at time throughout a Version.

[14] https://thedfirreport.com/2021/05/12/conti-ransomware/
[15] https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/