The First Step: Initial Access Leads to Ransomware

proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

June 14, 2021

Blog
Threat Insight
The First Step: Initial Access Leads to Ransomware

June 16, 2021 Selena Larson, Daniel Blackford, and Garrett G

Key Findings

- Preventing ransomware today largely has shifted from a direct email threat to an indirect threat where email is only part of the attack chain.
- Ransomware threat actors leverage cybercriminal enterprises – largely banking trojan distributors – for malware deployment. These access facilitators distribute their backdoors via malicious links and attachments sent via email.
- Banking trojans were the most popular malware distributed via email, representing almost 20% of malware seen in Proofpoint data the first half of 2021.
- Proofpoint currently tracks at least 10 threat actors acting as initial access facilitators or likely ransomware affiliates.
- Ransomware is rarely distributed directly via email. Just one ransomware strain accounts for 95% of ransomware as a first-stage email payload between 2020 and 2021.
- There is not a 1:1 relationship between malware loaders and ransomware attacks. Multiple threat actors use the same malware payloads for ransomware distribution.

Overview

Ransomware attacks still use email -- but not in the way you might think. Ransomware operators often buy access from independent cybercriminal groups who infiltrate major targets and then sell access to the ransomware actors for a slice of the ill-gotten gains. Cybercriminal threat groups already distributing banking malware or other trojans may also become part of a ransomware affiliate network. The result is a robust and lucrative criminal ecosystem in which different individuals and organizations increasingly specialize to the tune of greater profits for all—except, of course, the victims.

Preventing ransomware via email is straightforward: block the loader, and you block the ransomware.

Typically, initial access brokers are understood to be opportunistic threat actors supplying affiliates and other cybercrime threat actors after the fact, for example by advertising access for sale on forums. But for the purposes of this report, we consider initial access brokers to be the groups who obtain initial access via first-stage malware payloads and may or may not work directly with the ransomware threat actors.

These criminal threat actors compromise victim organizations with first-stage malware like The Trick, Dridex, or Buer Loader and will then sell their access to ransomware operators to deploy data theft and encryption operations. According to Proofpoint data, banking trojans – often used as ransomware loaders – represented almost 20% of malware observed in identified campaigns in the first half of 2021 and is the most popular malware type Proofpoint sees in the landscape. Proofpoint has also observed evidence of ransomware deployed via SocGholishwhich uses fake updates and website redirects to infect users, and via Keitaro traffic distribution system (TDS) and follow-on exploit kits which operators use to evade detection.

Proofpoint has unique visibility into initial access payloads – and threat actors that deliver them – often used by ransomware threat actors. It is important to note ransomware is not the only second-stage payload associated with the identified malware. In addition to email threat vectors, ransomware threat actors leverage vulnerabilities in software running on network devices exposed to the internet or insecure remote access services for initial access.

Map of the Ransomware Ecosystem

Proofpoint currently tracks around a dozen threat actors likely operating as initial access brokers, and many of the email threat campaigns distributing malware loaders observed by Proofpoint have led to ransomware infections. Confirmation of actor collaboration between access brokers and ransomware threat actors is difficult due to threat actors working hard to conceal their identity and evade detection. It is possible that initial access brokers and malware backdoor developers directly collaborate with – or operate as – ransomware-specific threat actors.

Initial Access Facilitators

The versatile and disruptive malware Emotet previously served as one of the most prolific distributors of malware enabling costly ransomware infections between 2018 and 2020. However, international law enforcement disrupted the malware in January 2021, wiping out its infrastructure and preventing further infections.

Since the Emotet takedown, Proofpoint observed consistent, ongoing activity from The Trick, Dridex, Qbot, IcedID, ZLoader, Ursnif, and many others in our data serving as first-stage malware payloads in attempts to enable further infections, including ransomware

attacks. Proofpoint tracks these malware families under the “banking” family. Over the last six months, banking trojans were associated with more than 16 million messages, representing the most common malware type observed in our data.

Additionally, Proofpoint tracks downloaders such as Buer Loader and BazaLoader that are often used as an initial access vector for ransomware attacks. In the last six months, Proofpoint identified almost 300 downloader campaigns distributing almost six million malicious messages.

Proofpoint researchers track backdoor access advertised on hacking forums from various threat actors. Depending on the compromised organization and its profit margins, access can be sold anywhere from a few hundred to thousands of dollars. Access can be purchased with cryptocurrency, most commonly bitcoin.

Proofpoint observes overlap between various threat actors, malware, and ransomware deployments. Our data and third-party reporting indicate for example, Conti ransomware has been associated with multiple first-stage loaders including Buer, the Trick, Zloader, and IcedID. IcedID has also been associated with Sodinokibi, Maze, and Egregor ransomware events.

TA800

TA800 is a large cybercrime actor Proofpoint has tracked since mid-2019. This threat actor attempts to deliver and install banking malware or malware loaders including The Trick, BazaLoader, Buer Loader, and Ostap. Its payloads have been observed distributing ransomware. Proofpoint assesses with high confidence TA800 is related to third-party reporting detailing BazaLoader implants that threat actors leveraged to distribute Ryuk ransomware.

TA577

TA577 is a prolific cybercrime threat actor tracked by Proofpoint since mid-2020. This actor conducts broad targeting across various industries and geographies, and Proofpoint has observed TA577 deliver payloads including Qbot, IcedID, SystemBC, SmokeLoader, Ursnif, and Cobalt Strike.

Proofpoint assesses with high confidence TA577 is associated with a March 2021 Sodinokibi ransomware infection. TA577 initially compromised the victim via emails containing malicious Microsoft Office attachments, which, when macros are enabled, download and run IcedID. Activity observed by this actor increased 225% in the last six months.

TA569

TA569 is a traffic and load seller known for compromising content management servers and injecting and redirecting web traffic to a social engineering kit. The threat actor leverages fake updates to prompt users to update their browser and download a malicious script. Proofpoint has tracked TA569 since 2018, but the actor has existed since at least the end of 2016.

Proofpoint assesses with high confidence TA569 is associated with WastedLocker ransomware campaigns that appeared in 2020 that leveraged the SocGholish fake update framework for ransomware distribution. Third-party entities associate this ransomware with a Russian cybercrime group known as Evil Corp. However, Proofpoint does not assess TA569 is Evil Corp.

TA551

TA551 is a threat actor tracked by Proofpoint since 2016. This actor frequently leverages thread hijacking to distribute malicious Office documents via email and demonstrates broad geographic and industry targeting. Proofpoint has observed TA551 distribute Ursnif, IcedED, Qbot, and Emotet.

Proofpoint assesses with high confidence TA551 IcedID implants were associated with Maze and Egregor ransomware events in 2020.

TA570

One of the most active Qbot malware affiliates, Proofpoint has tracked the large cybercrime threat actor TA570 since 2018. Qbot has been observed delivering ransomware including ProLock and Egregor. TA570 may use compromised WordPress sites or file hosting sites to host their payloads. TA570 has been observed conducting thread hijacking that distributes malicious attachments or URLs. In the last six months, TA570 activity is up almost 12%.

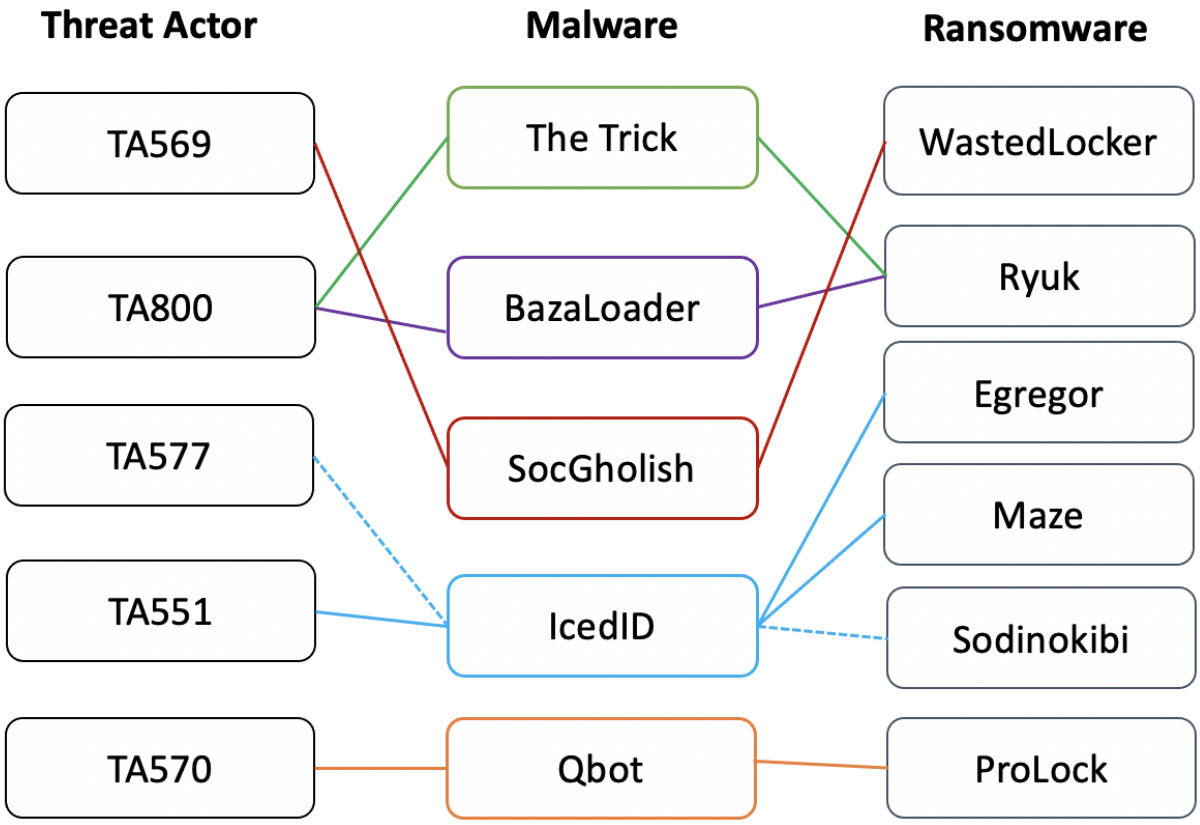

Figure 1: A sampling of observed threat actors, initial access payloads they delivered, and the associated ransomware deployed because of the initial access. Sourcing for these items is linked in the above descriptions for each actor.

TA547

TA547 is a prolific cybercriminal threat group primarily distributing banking trojans to various geographic regions including ZLoader, The Trick, and Ursnif. This actor often uses geofencing, so payloads may not be accessible to users in all regions. Attempts to access payloads from VPNs are also often unsuccessful since the actor blacklists VPN exit IP addresses. Over the last six months, the number of identified campaigns from this actor spiked almost 30%.

TA544

This high-volume cybercriminal threat actor regularly installs banking malware and other malware payloads, various geographic targeting including Italy and Japan. This threat actor is likely a malware affiliate working with different developers. TA544 has been observed distributing Ursnif and Dridex trojans and has sent over eight million malicious messages in the last six months according to Proofpoint campaign data.

TA571

Since 2019, Proofpoint has tracked TA571 and its attempts to distribute and install banking malware. This actor distributes Ursnif, ZLoader, and Danabot and often uses legitimate file hosting services or compromised or spoofed infrastructure for payload hosting. Typically, TA571 distributes more than 2,000 messages per campaign.

TA574

Proofpoint researchers observed TA574 distribute over one million messages in the last six months according to campaign data. This high-volume cybercrime threat actor conducts broad industry targeting and attempts to deliver and install malware including ZLoader. Typically, this group distributes malicious Office attachments and leverages some techniques including geotargeting and detecting User Agents before malware is deployed. Proofpoint researchers have tracked TA574 since June 2020.

TA575

TA575 is a Dridex affiliate tracked by Proofpoint since late 2020. This group distributes malware via malicious URLs, Office attachments, and password-protected files. On average, TA575 distributes almost 4,000 messages per campaign impacting hundreds of organizations.

First-Stage Ransomware

Proofpoint still sees ransomware distributed via email directly, as attachments or links in email, at considerably lower volumes. For example, in 2020 and 2021 Proofpoint identified 54 ransomware campaigns distributing just over one million messages.

Of these, Proofpoint identified four Avaddon campaigns containing about a million messages in 2020, representing 95% of the total. In May 2021, the U.S. Federal Bureau of Investigation released details on an increase in Avaddon activity, noting the ransomware operators obtained initial access via remote access portals such as RDP and VPN, a pivot away from direct email access. This operational shift is consistent with Avaddon campaigns observed in Proofpoint data.

Other ransomware leveraging email directly as an access vector and have appeared in Proofpoint data this year include Hentai OniChan, BigLock, Thanos, Demonware, and Xorist.

Diversification of the Criminal Enterprise

Proofpoint's Threat Research team analyzed data from 2013 to present to better understand observed trends associated with ransomware and email as an initial access vector. Proofpoint observed that ransomware campaigns distributed directly via email as attachments or links occurred at relatively low, consistent volumes before 2015, at which

point threat actors began distributing ransomware via email at considerably higher volumes. Threat actors would send large numbers of messages to individual email addresses containing the malicious files or URLs that would infect the victim when clicked on or downloaded. Locky, for example, was sent in as many as one million messages per day in 2017 before its operations abruptly stopped.

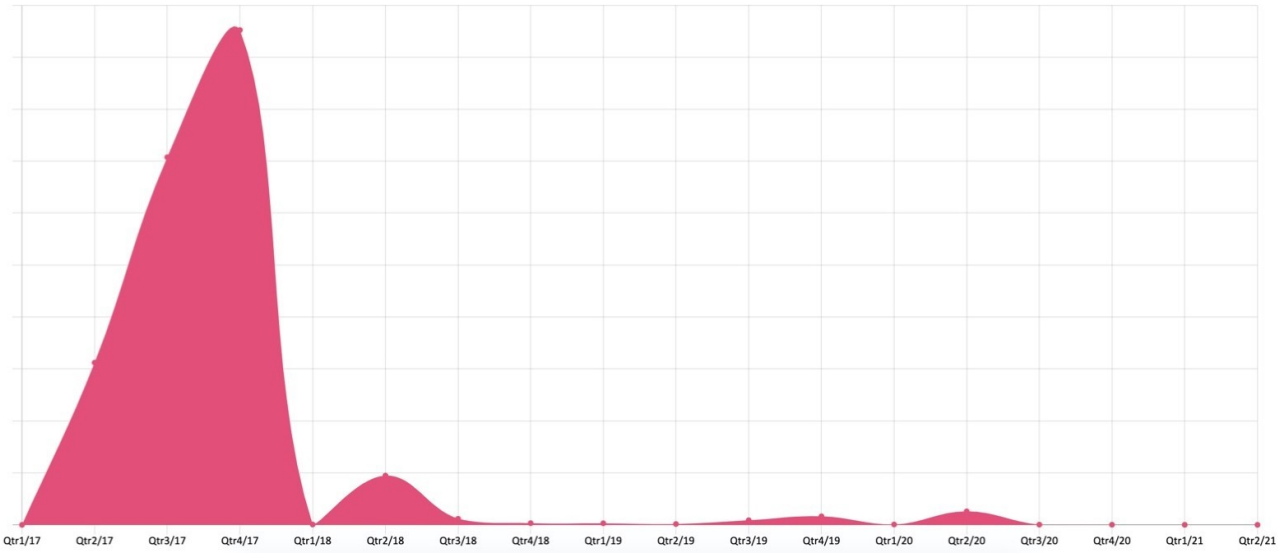

Figure 2: Ransomware volumes as a first-stage malware

Proofpoint data shows a significant drop in first-stage ransomware campaigns in 2018. Multiple factors contributed to the pivot away from ransomware as a first-stage payload, including improved threat detection, individual encryption activities resulting in limited payouts, and the introduction of wormable and human-operated threats that had exponentially more disruptive capabilities.

How Hackers Hunt

Ransomware threat actors currently carry out “big game hunting,” conducting open-source surveillance to identify high-value organizations, susceptible targets, and companies’ likely willingness to pay a ransom. Working with initial access brokers, ransomware threat actors can leverage existing malware backdoors to enable lateral movement and full domain compromise before successful encryption.

An attack chain leveraging initial access brokers could look like this:

1. A threat actor sends emails containing a malicious Office document
1. A user downloads the document and enables macros which drops a malware payload
1. The actor leverages the backdoor access to exfiltrate system information
1. At this point, the initial access broker can sell access to another threat actor

1. The actor deploys Cobalt Strike via the malware backdoor access which enables lateral movement within the network

1. The actor obtains full domain compromise via Active Directory

1. The actor deploys ransomware to all domain-joined workstations

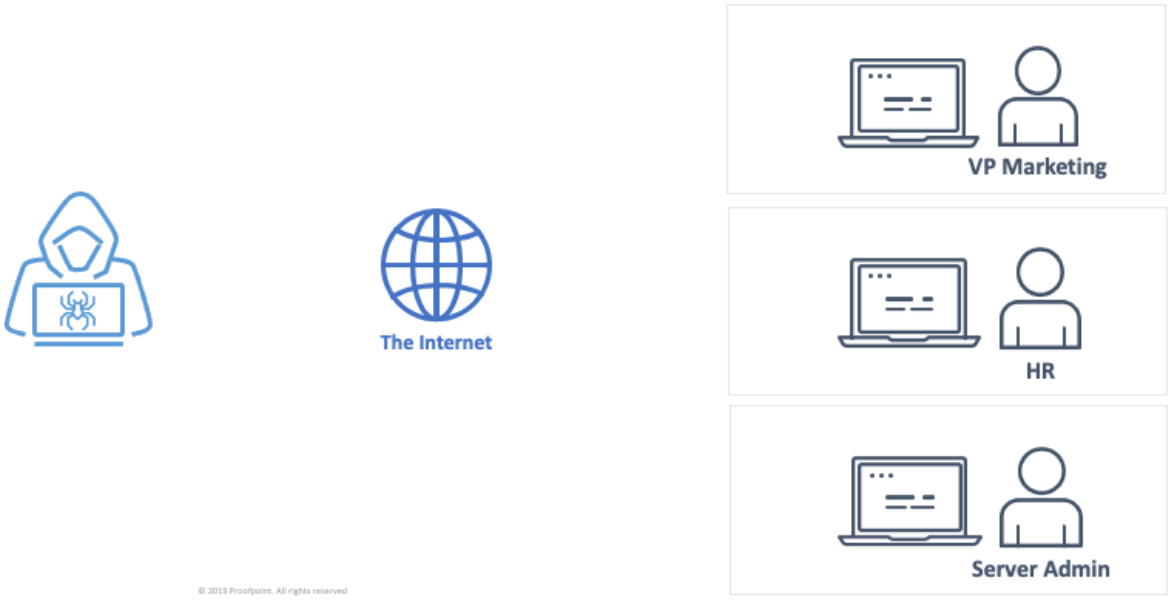

Figure 3: Sample attack chain via initial access broker

Outlook

So far in 2021, Proofpoint continuously observes email-based threats including downloaders and bankers with multi-stage payloads that often lead to ransomware infections. The threat actors are conducting extensive reconnaissance, privilege escalation, and lateral movement within the environment before manually deploying the ransomware payload. One key metric to watch is dwell time. Over the last two years, multiple public reports from incident response companies point to a decrease in the amount of time threat actors spend within an environment before encryption activities. Some incidents are reporting two-day infection timelines between initial access and ransomware deployment compared to reported averages of 40 days in 2019.

Short dwell times, high payouts, and collaboration across cybercriminal ecosystems have led to a perfect storm of cybercrime that the world's governments are taking seriously. In response to recent high-profile ransomware attacks, the United States government proposed new efforts to combat ransomware, and it was a hot topic at

the 2021 G7 conference. It is possible with new disruptive efforts focused on the threat and growing investments in cyber defense across supply chains, ransomware attacks will decrease in frequency and efficacy.

Learn more about ransomware attacks and prevention.

Subscribe to the Proofpoint Blog