BITSIGHT
The Standard in SECURITY RATINGS

WHITE PAPER

Identifying Unique Risks Of Work From Home-Remote Office Networks

Introduction

During the period of March 2020, we looked at a sample size of **41,000 US-based organizations** to understand the difference between corporate networks and Work From Home-Remote Office (WFH-RO) networks from a cyber risk perspective.

Some attributes of WFH-RO networks include:

Malware

- **3.5 times more likely** than corporate networks to have at least one family of malware
- **7.5 times more likely** to have at least five distinct families of malware
- Common families of malware are extremely prevalent including **Mirai**, which is observed **20 times more frequently**, and **Trickbot**, which is observed **3.75 times more frequently**

Services and Remote Management Exposure

- **More than 25 percent** of all devices have one or more services exposed on the Internet
- **Almost one in seven** WFH-RO IP addresses have exposed cable modem control interfaces

In this white paper, we take a closer look at corporate-associated residential IP addresses (WFH-RO IPs) and discover attributes that pose unique cybersecurity risks as compared to in-office corporate networks.

With companies around the world adapting to a remote workforce in an expedient manner, we wanted to understand any inherent and unconsidered risks posed to those organizations due to the home environment. We isolated the study to the assessment of the network perimeter of devices on those networks and researched the differences in the distribution of compromised systems observed on those networks on a sample of 41,000 US-based organizations.

In order to perform this study, we first had to construct the asset maps of WFH-RO IP addresses associated with each company programmatically. Since BitSight evaluates the externally observable security performance of organizations across many industries around the world, we already had the corresponding maps of assets directly controlled and associated with organizations.

We enriched the WFH-RO maps using the same aforementioned telemetry that we continuously gather to assess corporate cybersecurity hygiene as data points for this study.

25.2 percent of WFH-RO IP addresses have one or more services exposed on the Internet.

Key Findings

The following were among the key findings of the study:

1. **As the number of employees and home IP addresses associated with an organization scales, the diversity of threats that their devices are exposed to on the local home network rapidly expands with it.**

   During the period of March 2020:

   - **13.3 percent** of companies had at least one observation of a malware family on their corporate network for the families we observe, while **45.0 percent** of companies had at least one observation of malware family on their WFH-RO networks, making them 3.5 times more likely to have a malware infection present.
   - **2.3 percent** of companies had observations of at least five distinct families on their corporate network while **17.3 percent** of companies had at least five distinct families observed on their WFH-RO networks.

2. **Residential networks exhibit their own unique attack surfaces with regards to network perimeter security. 25.2 percent of WFH-RO IP addresses have one or more services exposed on the Internet.**

   Of those 25.2 percent:

   - **61.2 percent** of WFH-RO IP addresses that have one or more services open have an exposed cable modem control interface, either through the TR-069/TR-064 protocols or other remote management functions, which have been an exploitation channel used by Internet-wide attacks in recent years.[1] Against the wider population, this amounts to 15.3 percent of all corporate-associated residential IP addresses.
   - At least **9.5 percent** of WFH-RO IP addresses that have one or more services open have an exposed web administrative interface for their cable modems, routers, cameras, storage, and other IoT devices. Considering most of these interfaces are inadvertently accessible or infrequently updated by the user, they pose a significant risk in the days of IoT device exploitation through such channels.[2] This amounts to at least **2.4 percent** of all WFH-RO IP addresses.

3. **Corporate devices will be facing new risks of network compromise due to a higher population of malware that is more prevalent on residential networks.**

   These malware families will pose a greater threat to devices whose operating environment relied on an over-emphasis on physical-based network controls.

For example:

- Mirai[3] is observed at least **20 times more frequently** on WFH-RO networks than corporate networks
- Trickbot[4] is observed at least **3.75 times more frequently** on WFH-RO networks than corporate networks

The move of corporate managed assets into largely unmanaged environments with its attendant increase in local threats brings challenges to security practitioners. Employee education may be the best approach to maintaining adequate security.

WFH-RO IP Addresses

Corporate-associated home office networks are **3.5 times** more likely to have at least one malware infection.

To perform this study, we had to discover the set of remote IP addresses used by the employees of each organization. To drive its security ratings product, BitSight already has a set of high-quality, up-to-date maps of corporate network assets including those self-hosted and in the cloud.

These maps are constructed and maintained primarily via automated processes with constant feedback from human intelligence to improve the automation.

We used an extension of these processes to find additional IP addresses used by employees working at home or in remote offices by investigating the ecosystem of devices observed on corporate networks and finding their most closely associated non-corporate networks via session identifiers and device behaviors.

Once that process is completed, we are left with a set of IP addresses for each organization representing a sample of associated residential networks that fit the criteria for this study. We term that set of IP addresses for each organization as their corresponding WFH-RO asset map.

There are many sources of noise that complicate the discovery of associated residential networks, which if introduced into the resulting asset maps, can cause significant skews in findings and results. These sources can include IP addresses used by cellular networks, carrier-grade Network Address Translation (NATs) serving many consumer networks, or common access points such as Internet cafes or transient access services such as hotels and airports.

One input of how we measure risk for our BitSight Security Ratings is to assess the distribution of Internet-facing workstation and mobile operating systems in-use at organizations. We not only look at the mere presence of the operating system of Internet-facing assets (e.g., the use of Windows XP) but we also model the number of systems using that operating system (i.e., the presence of an estimated 1,000 Windows XP machines is more notable from a risk perspective than an estimation of a single Windows XP machine).

The more prevalent an out-of-date operating system is within an organization, as well the number of distinct out-of-date versions, is a telling insight into the security controls and practices at a company. We used the foundation of these principles and models into order to improve the quality of the WFH-RO network asset maps significantly.

The graph in *Figure 1* is a visual representation of how the individual WFH-RO IP addresses are connected with the corporate network after the noise-reduction process has completed. The IP addresses directly managed by the company are highlighted in blue while the black nodes represent WFH-RO IP addresses associated with that organization. The lines in between the nodes represent the relationships identified between those IP addresses.

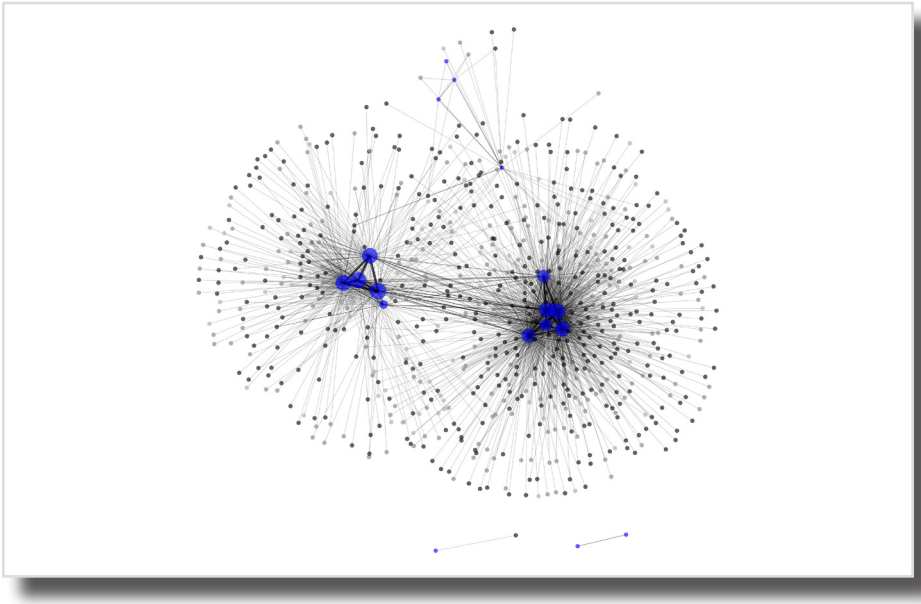


Figure 1. Connections to the Corporate Network
A visual representation of how the individual WFH-RO IP addresses are connected with the corporate network after the noise-reduction proceess has completed. (WFH-RO IP addresses are in black, corporate-managed IP addresses are in blue.)

Depending on the organization, IP addresses can be seen to be clustered by geographic location of the physical office locations.

Other more centralized corporate networks, or those without a large physical footprint, resemble more straightforward spoke-hub graph representations, as shown in a larger organization (see *Figure 2*).

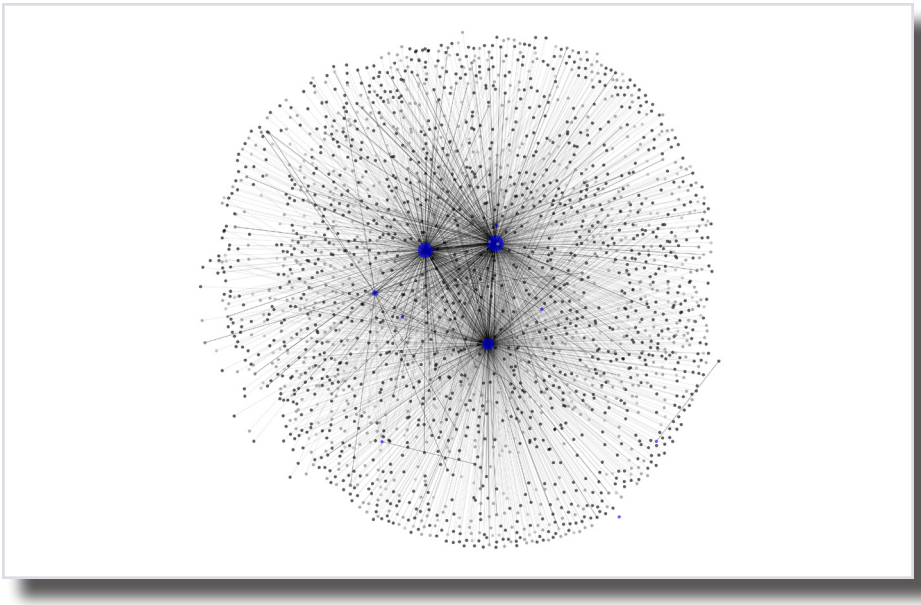


Figure 2. Centralized Connections
Centralized corporate networks, or those companies without a large physical footprint, resemble more straightforward spoke-hub representations. (WFH-RO IP addresses are in black, corporate-managed IP addresses are in blue.)

Network Perimeter

The network perimeter and subsequent access control layers[5] are one of the most closely managed and watched elements of a comprehensive security and network operations program.

The first artifact we wanted to understand was how the perimeter attack surface differed between work from home-remote office networks and their corresponding corporate offices.

When we assess the perimeter of these corporate-associated residential IP addresses, we find that **25.2 percent** of them have one or more services exposed on the Internet.

The bar chart in *Figure 3* shows the distribution of ports and services across IP addresses belonging to corporate networks and IP addresses belonging to WFH-RO networks. The port and service counts are normalized by the total number of IP/service pairs for each category in order to highlight the differences in the distributions between the two types.

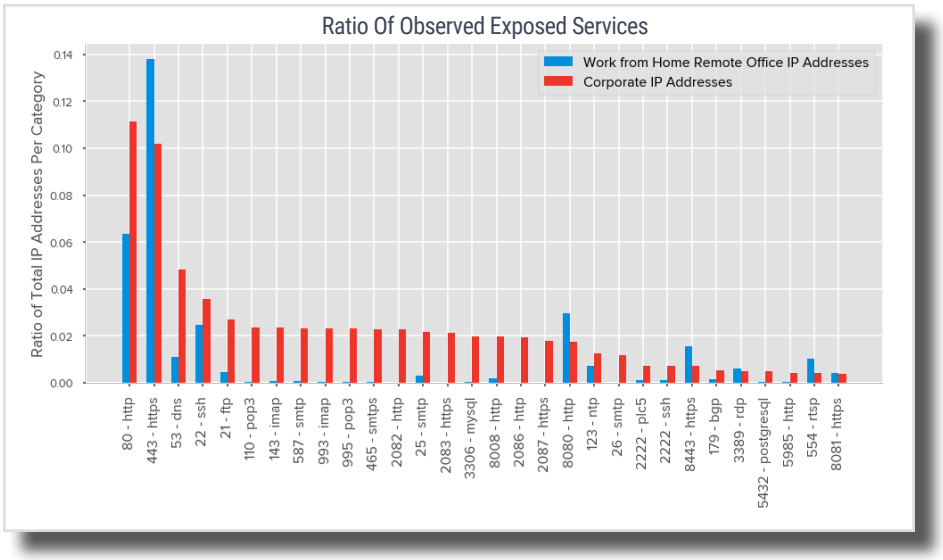


Figure 3. Ratio of Observed Exposed Services
This bar chart highlights the differences in the distribution of ports and services between IP addresses belonging to corporate networks (in red) and IP addresses belonging to WFH-RO networks (in blue).

From this chart, there are a few notable observations:

1. As one would expect, corporate networks have a significantly higher relative number of systems self-hosting email-related services, such as SMTP, POP3, IMAP and its TLS-protected equivalents. These services are close to non-existent on WFH-RO networks. In fact, some consumer Internet Service Providers block or simply inhibit residential networks, including some of their small business customers, from self-hosting email[6] in order to reduce the probability of spam originating from their networks.

2. Other services, such as the web service for cPanel, Web Host Manager (WHM), and WebMail administrative interfaces commonly observed on ports 2082 & 2083, 2086 & 2087, and 2095 & 2096 respectively also are almost exclusively observed on company networks.
3. Likewise, other protocols, such as those associated with SSH and databases have a very minor presence on WFH-RO networks but are observed more extensively on corporate networks.

Another way of looking at this distribution is to show the most relative prevalent services exposed on WFH-RO networks in comparison to company networks, as shown in the bar chart in *Figure 4*:

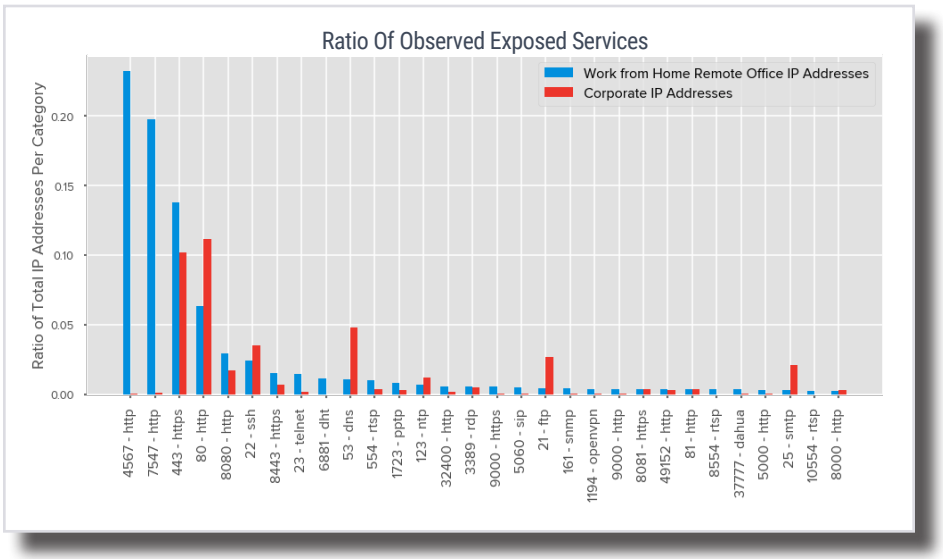


Figure 4. Exposed Services
This bar chart highlights the most relative prevalent services exposed on WFH-RO networks in comparison to company networks.

From this chart, there are also a number of notable observations:

1. WFH-RO networks have a much higher prevalence of modem and router management protocols typically enabled by default on many consumer modems, most often provided to consumers by their ISP, such as TR-069 and TR-064 protocols operating on port 7547 and other customer-premise equipment remote management protocols as also observed on port 4567. These make little appearance on company networks as organizations often control the hardware for their egress Internet services and subscribe to different services.

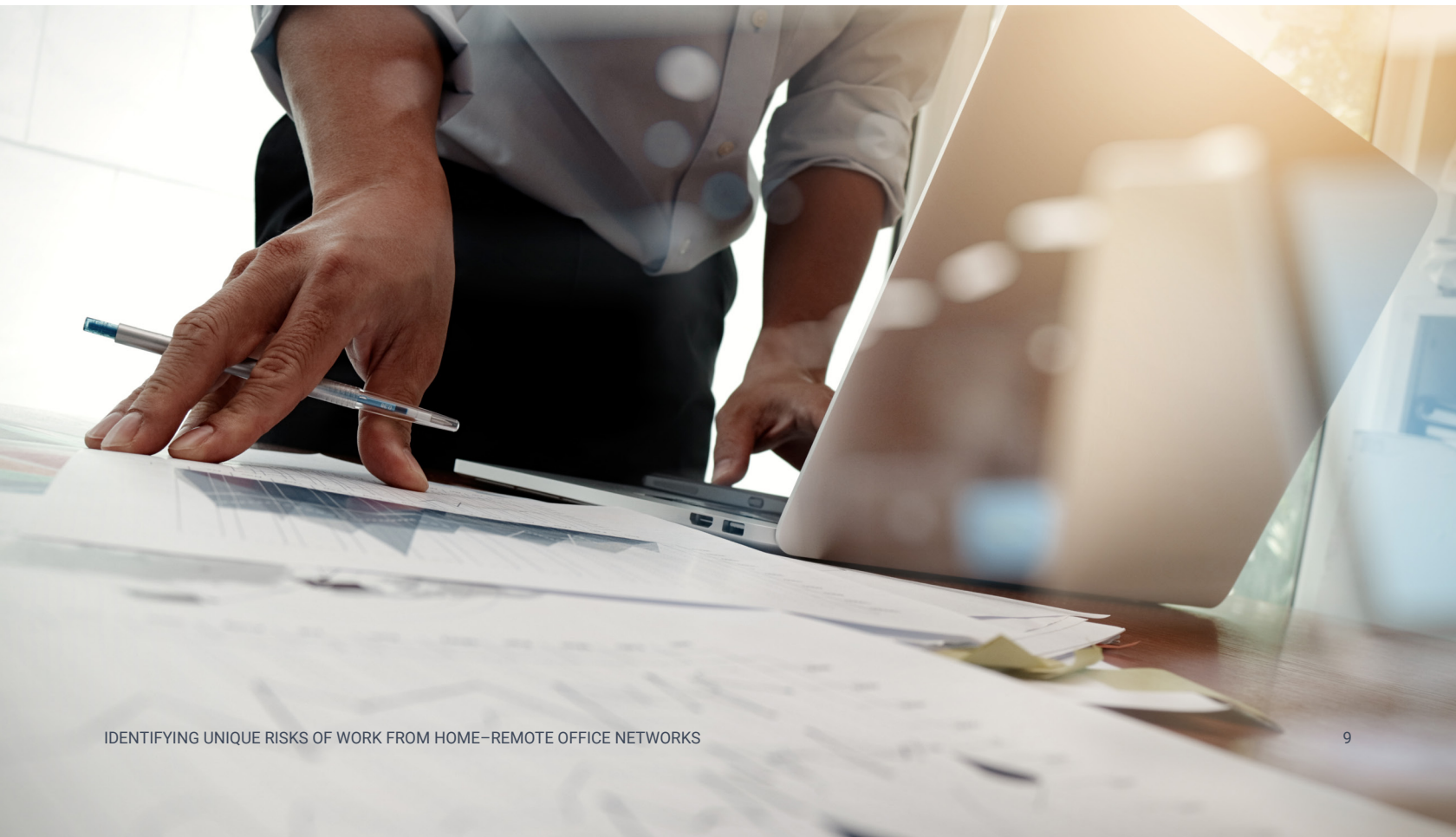
   15.4 percent of WFH-RO IP addresses have exposed cable modem control interfaces when you include the IP addresses that do not have any service exposed. This number increases further when HTTP-based control interfaces are taken into account.
2. On the other hand, web-based services also commonly are exposed on these networks, and while inherently they are not a negative observation, the purpose of these web services is an important artifact to understand. We can also see in the chart above that port 8080 and 8443 are more

15.4 percent

of WFH-RO IP addresses have exposed cable modem control interfaces when you include the IP addresses that do not have any service exposed.

common in relative terms. In fact, of the WFH-RO IP addresses that have a web service exposed, at least **22 percent** of those are a consumer modem or router administrative interface.

3. Devices participating in BitTorrent activities (port 6881) are much higher relative to company networks. One of the reasons we assess illegitimate file sharing as part of the BitSight Security Rating is due to the increased exposure organizations face through permitting this activity.
4. There is a higher relative prevalence of Real-Time Streaming Protocol (RTSP) on residential networks, a protocol for video streaming, in comparison to company networks. In context to residential networks, this is not the protocol associated with common video streaming services such as YouTube, Netflix, or Twitch, but the protocol used by IoT devices such as cameras.
5. Telnet is more prevalent on WFH-RO networks when compared to corporate networks due to remote interfaces being accessible on home consumer routers. Telnet is an old remote access protocol that often is accessible inadvertently on many IoT devices with little value provided back to the user, especially residential networks, as it has been a channel of attack for many years.[7]



Compromised Systems

Of the WFH-RO IP addresses that have a web service exposed, at least **22 percent** of those are a consumer modem or router administrative interface.

The presence of compromised devices on corporate networks is strong evidence of poor security hygiene or failed controls, particularly on endpoint workstations whose risk often is concentrated in the maturity and configuration of the endpoint protection technologies federated across the operating system protecting that device, as well the education and knowledge distilled into the individual users of those devices.

For these reasons, we continuously research and monitor the devices infected by botnets associated with currently more than 250 active malware families spread across the world.

This wide visibility into infected systems forms a core component of how we measure the cybersecurity posture of organizations.

We previously reported that we observe approximately 90 perent of malware infections on service provider networks. That research, however, did not explore the differences between security controls on corporate networks, as compared to associated home networks.

Unlike the analysis of the network perimeter where we had collected all corporate assets into one group and the WFH-RO IP addresses into another group, we split those assets into independent maps based on companies.

More specifically referring back to the graphs in *Figures 1 and 2*, for each organization we treat all the blue nodes as representative of the corporate company map, or "corporate networks," while we treat all black nodes as representative of the "WFH-RO networks," and treat each group as a single entity. Each company thus has a map representing its corporate assets and another map representing its WFH-RO assets.

With this in mind, we can compare the malware behavior between those two groups for each company, as well as the wider population, by joining our compromised systems telemetry from March 2020 onto these asset maps.

The scatter plot in *Figure 5* shows the distribution of companies and their respective family counts between both of their asset types. Each family is counted only once when it is observed during this period, even if it affects multiple devices or occurs across multiple days. Each dot represents a single company in the study.

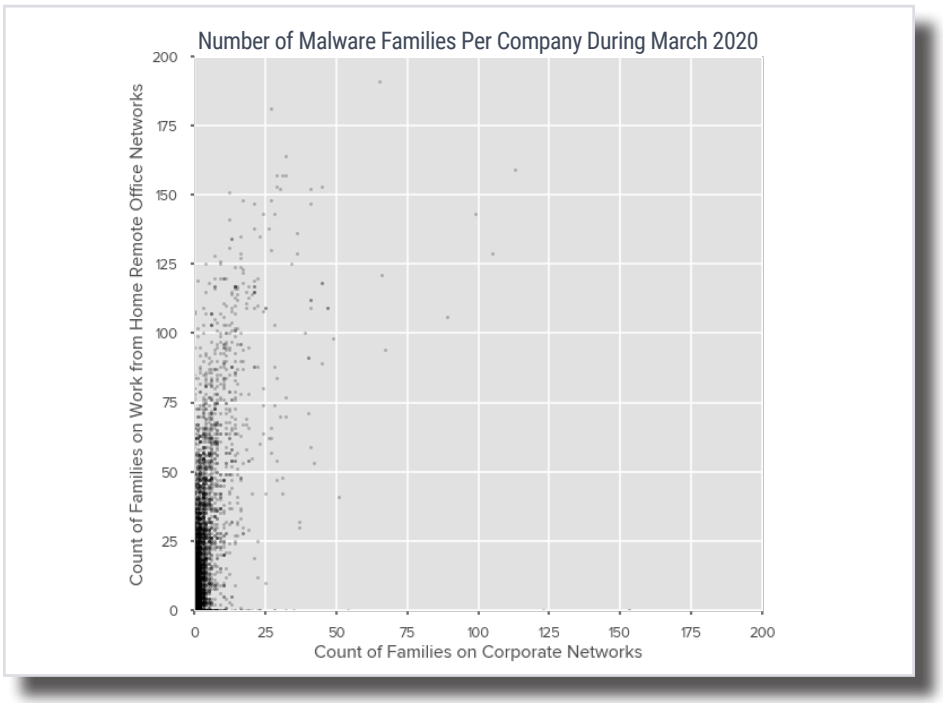


Figure 5. Number of Malware Familes Per Company
17.3 percent of companies had at least five distinct families of malware observed on their WFH-RO networks.

During this period:

- **13.3 percent** of companies had at least one observation of a malware family on their corporate network for the families we observe, while **45.0 percent** of companies had at least one observation of malware family on their WFH-RO networks.
- **2.3 percent** of companies had observations of at least five distinct families on their corporate network while **17.3 percent** of companies had at least five distinct families observed on their WFH-RO networks.

As the number of WFH-RO IP addresses associated with a company increases, we observe more unique malware families on both the WFH-RO networks and the corporate networks (see *Figure 6*).

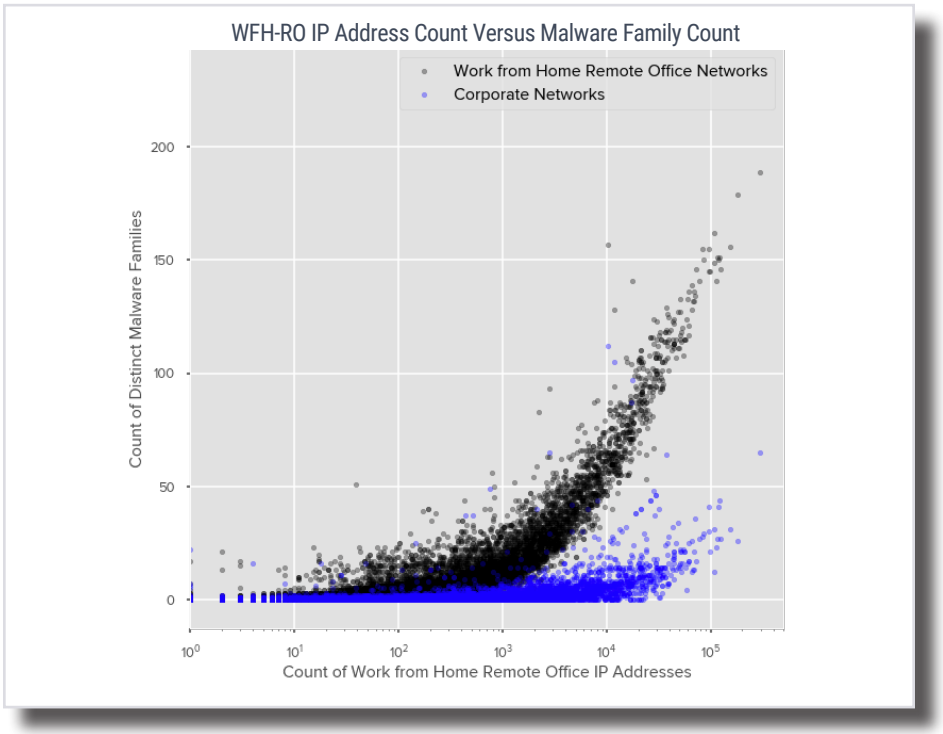


Figure 6. WFH-RO IP Address Count vs. Malware Family Count
As the number of WFH-RO IP addresses associated with a company increases, we observe more unique malware families on both the WFH-RO networks and the corporate networks.

This relationship reflects the fact that the count of home IP addresses acts as a rough proxy for the size of an organization.

As the size of the organization increases, so does its complexity at managing infrastructure, processes, and human practices within the physical and digital boundary of the corporate network.

The size of the organization, however, also has a much more rapid relationship to the diversity of malware families that their assets are exposed to outside the corporate network and in residential networks.

The second component we wanted to investigate was the characteristics of the individual malware families. More specifically, we wanted to determine whether there are families that are observed more frequently on residential networks and less likely on corporate networks and vice-versa.

The plot in *Figure 7* shows the number of company asset maps that each family was observed on, with the Y-axis representing the count of WFH-RO networks and the X-axis representing the count of corporate networks.

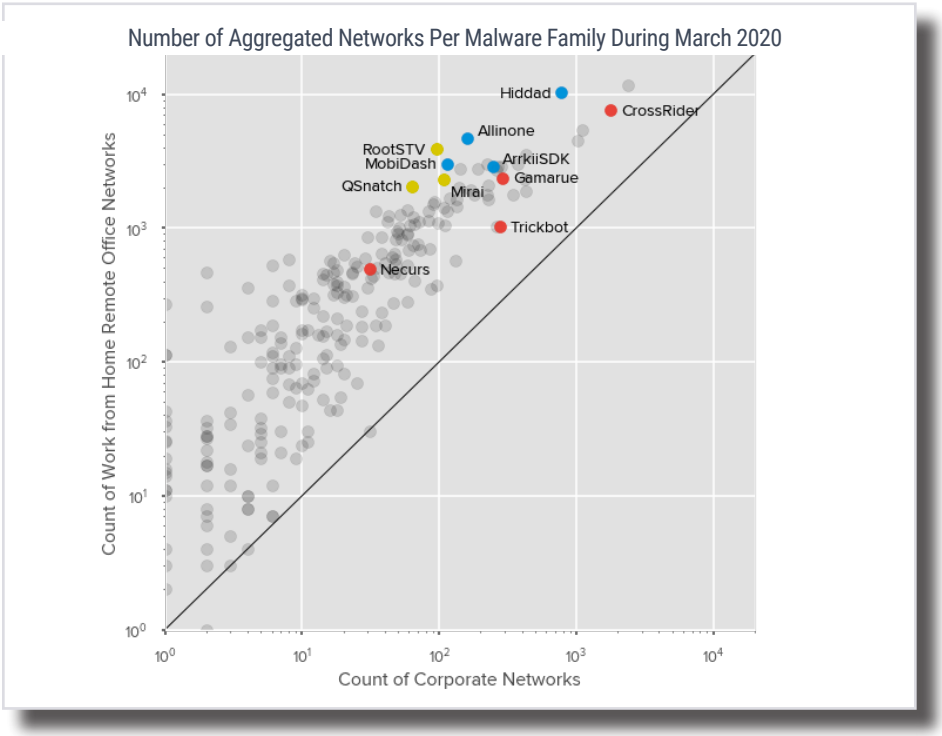


Figure 7. Aggregated Networks Per Malware Family
In general, every malware family was observed more frequently on WFH-RO than on their corporate network counterparts.

In general, every family was observed more frequently on WFH-RO than on their corporate network counterparts.

As malware families drift away from the center line towards the top-left they generally appear more frequently on consumer networks while those families that are further to the bottom-right have a tendency to be seen relatively more on organizational networks.

These preferences generally are representative of the types of devices and software that these malware families target, and we see this reflected in the frequency and infection targets of those families:

- The examples highlighted in blue are malware families and potentially unwanted applications affecting mobile platforms (Hiddad,[8] Mobidash,[9] ArrkiiSDK). The types of devices these families target often rely upon users running older devices, or following poor security practices, such as side-loading applications, which might be prohibited on corporate devices managed by MDM solutions with stricter policies.[10]

17.3 percent
of companies had at least five distinct families of malware observed on their WFH-RO networks.

- The examples highlighted in yellow are those that target IoT devices (Mirai[3] and RootSTV[11]) or consumer devices (QSnatch[12]). While corporate devices have their share of IoT devices present, they often are better managed than those owned and operated by consumers. Mirai gained prominence and its effectiveness not from its rapid exploitation of a new vulnerability, but in part from taking advantage of devices in default states or other devices with poor configurations.[13]
- The examples highlighted in red are those affecting Windows platforms (CrossRider,[14] Trickbot,[4] Necurs) which have a higher prevalence in corporate networks compared to the other two sets.

These characteristics give us visibility on the likelihood of the environment for which we would observe a given family.

For example, **Mirai** is observed at least **20.1 times more frequently** on WFH-RO networks than corporate networks, **QSnatch** is observed **29.7 times more frequently** on WFH-RO networks, while **Necurs** and **Trickbot** are observed at least **13.8 and 3.8 times more frequently** on WFH-RO networks than corporate networks respectively.

Conclusion

While the notion of a single trusted network that corporate workstations operate in exclusively has been fading over the last decade, there certainly are challenges that organizations are going to face who have not dealt with such diverse environments.

Given the circumstances of the last several months, these devices now have moved abruptly into environments with a different set of unique entries into the local network on a persistent basis, and organizations should be aware that their cybersecurity policies, practices, and education should be aligned with these new operating environments.

Worms, particularly those that have been developed as ransomware, have become a recent concern among many practitioners and network operators, due to the ability to spread onto unpatched systems once they gain entry to the local network. The success of these families infecting many other systems internally reflect the disparity of attention paid to the corporate perimeter versus the health of the individual workstations and endpoints.

Defense-in-depth strategies also now are more complicated and difficult to implement as security and network operation teams already had to balance the technology and configurations they deploy against the freedom that the various functional teams at companies need to be successful.

Recommendations

From this study, and as the course of general best practices, the following set of recommendations are put forward:

1. **Reduce over-dependence on a local trusted network and physical-based network controls.**
   Companies and organizations who have focused much of their security-based program on the perimeter should ensure they invest in technologies and operations that better harden the workstation, services, and sensitive data while still enabling the business to be successful remotely. Organizations that already have adopted the zero trust security model[15] into their culture and security programs likely will see the least change in their threat model.
2. **Improve and execute on patch management programs for both workstations and servers.**
   New vulnerabilities will continue to be discovered, published, and weaponized throughout the next several months and it will be as important now as it was historically to continue to update and patch systems that might now be more vulnerable to attack.

Malicious actors will capitalize on the fear around COVID-19. Users should be educated and reminded continuously of the methods that use *them* as a vector of attack.

3. **Continue user education and training.**
   Malicious actors will capitalize on the fear around COVID-19 and users should be educated and reminded continuously of the methods that use them as a vector of attack.
   - Make them aware that these threats and best practices extend beyond the corporate network and into the home.
   - Encourage users to also follow best practices offered by manufacturers of their own personal devices to further limit the attack surface exposed to corporate devices.
   - Consider sharing specific recommendations and best practices directly with employees.

Interested in learning more about mitigating cybersecurity risk across a remote workforce? Check out our remote office risk infographic and explore our additional COVID-19 resources.

REFERENCES

1 https://arstechnica.com/information-technology/2016/11/notorious-iot-botnets-weaponize-new-flaw-found-in-millions-of-home-routers/
2 https://www.tomsguide.com/news/coronavirus-router-hack
3 https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html
4 https://blog.malwarebytes.com/101/2018/11/trickbot-takes-top-business-threat/
5 https://www.cisecurity.org/controls/boundary-defense/
6 https://www.xfinity.com/support/articles/email-port-25-no-longer-supported
7 https://securityintelligence.com/telnet-an-attackers-gateway-to-the-iot/
8 https://www.avira.com/en/blog/top-rated-android-malware
9 https://blog.malwarebytes.com/cybercrime/2018/07/mobile-menace-monday-adware-mobidash-gets-stealthy/
10 https://insights.samsung.com/2019/11/26/what-are-the-risks-of-sideloaded-android-applications/
11 https://blog.trendmicro.com/trendlabs-security-intelligence/android-based-smart-tvs-hit-by-backdoor-spread-via-malicious-app/
12 https://www.kyberturvallisuuskeskus.fi/en/news/qsnatch-malware-designed-qnap-nas-devices
13 https://en.wikipedia.org/wiki/Mirai_(malware)#Malware
14 https://securityboulevard.com/2019/08/crossrider-adware-still-causing-unwanted-mac-browser-redirects/
15 https://en.wikipedia.org/wiki/Zero_Trust

Achieve continuous visibility into your digital ecosystem with BitSight Attack Surface Analytics.

Learn More.
www.BitSight.com/attack-surface-analytics

BITSIGHT®
The Standard in SECURITY RATINGS

111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight
BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to analyze vast amounts of data on security issues continuously. Seven of the top 10 largest cyber insurers, 25 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit www.BitSight.com, read our blog, or follow @BitSight on Twitter.