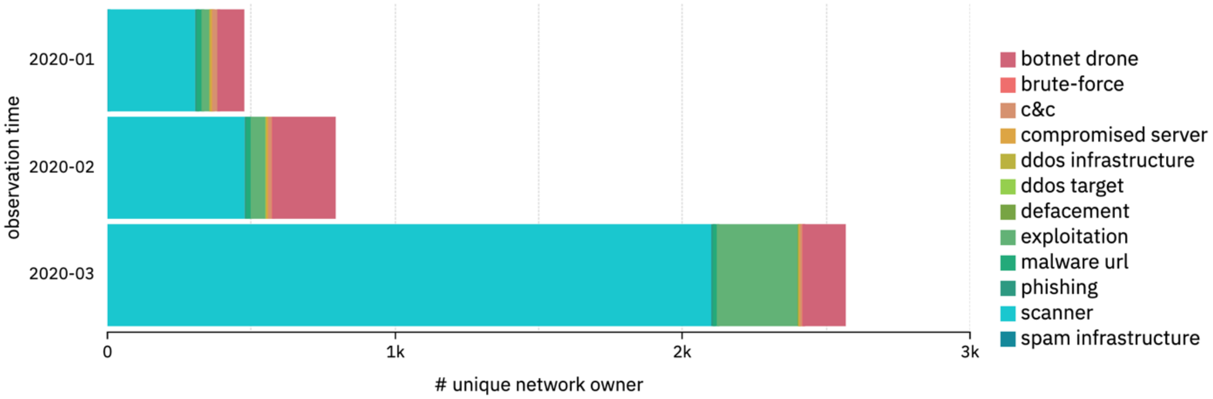
APRIL 17th, 2020

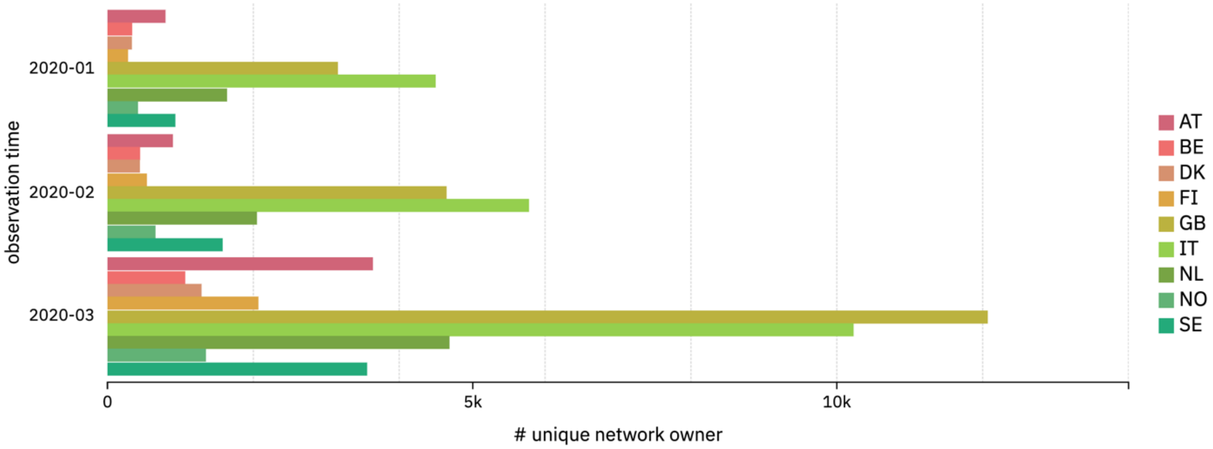
# Number of Potentially Compromised Organizations More than Doubles Since January

At the end of March, Arctic Security, a Finnish company, noticed an uptick in the number of organizations being potentially compromised on a weekly basis in Finland. During a normal week, the number for a small country such as Finland is approximately 200 organizations. For the week starting on Monday 2020-03-16, the number of organizations had suddenly jumped to 800.



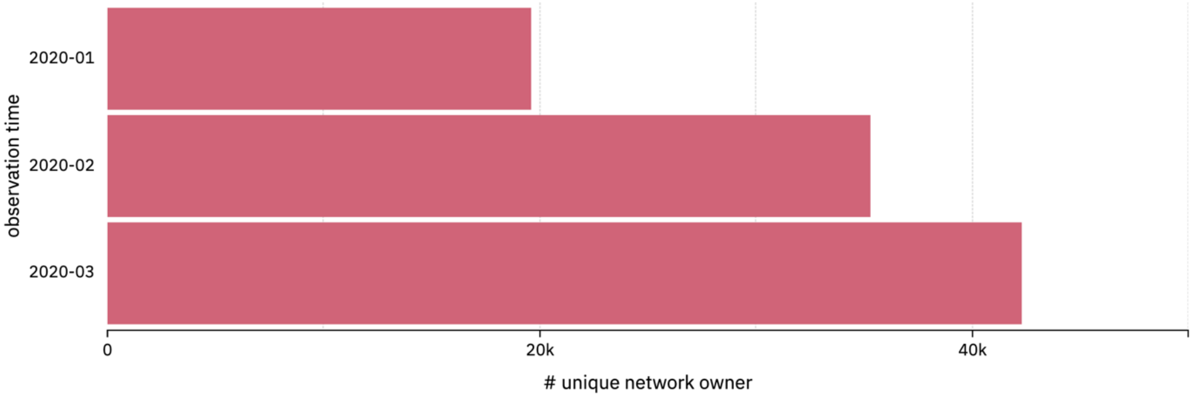
**Potentially compromised organizations more than doubled in Finland between January and March.**

Digging deeper into the issue, Arctic Security quickly discovered that looking at the same data on a monthly basis, the increase had been quite substantial between January and February and yet again between February and March. Trying to understand, whether this rise in affected organizations was not just happening in Finland, we pivoted the same parameters for 8 other European countries: Sweden, Norway, Denmark, Netherlands, Belgium, UK, Austria and Italy.



**Significant increase in potentially compromised organizations across 9 European countries.**

Looking at the US., the same trend of potentially compromised organizations was evident across all countries, and the results are worrying.



**Between January and March, potentially compromised organizations in the US doubled.**

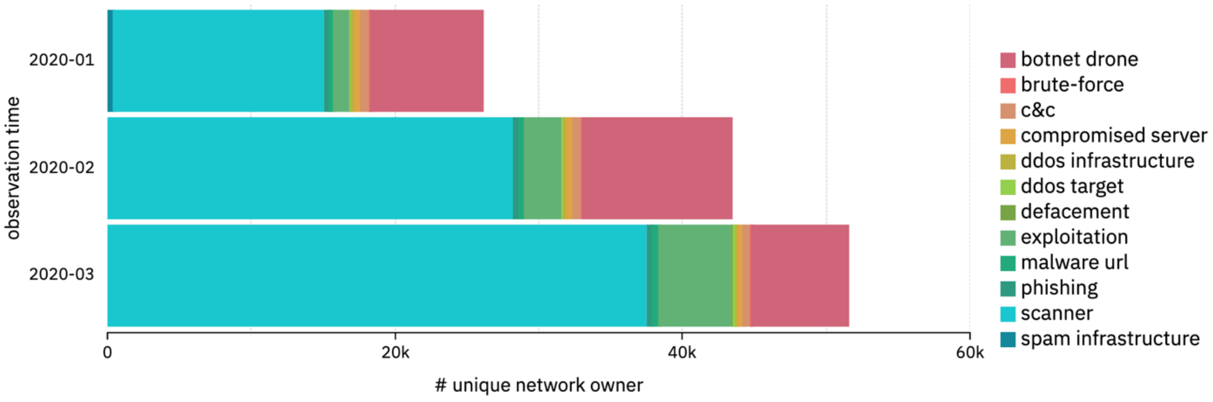
Rather than looking at the number of individual IP addresses (devices) that were compromised, which is a common approach, Arctic Security gained a bird's eye view of the Internet using Team Cymru's global cyber intelligence data. Rather than a curated list of "known bads", Team Cymru's data gives analysts access to what they refer to as pure signal, which allowed Arctic Security to map these potential threats at the network owner level. In this context, a network owner roughly equates to an organization, such as a private company or a public sector agency.

"Analysts looking for an increase in the number of compromised IPs or an increase in the number of observed compromises per IP will not see a marked increase," commented Lari

Huttunen, Senior Analyst with Arctic Security. “However, the number of malicious connections to the Internet coming from organizations has increased, and only Team Cymru was able to show us this differential.”

So, what does this mean?

Reaching out to informed peers for a potential explanation, we jointly agreed that there seems to be a strong correlation between the numbers and the increase in remote workers. The week the uptick happened in Finland, the government had issued a strong recommendation for people to stay home and work. Likewise, all other countries observed had issued stay-at-home guidance. This means the number of people using a VPN to connect to their companies’ systems have increased by orders of magnitude. One cannot say with certainty what causes organizations to get compromised while most workers are working from home. However, it seems that the connections normally blocked by on-premises security solutions do not work as well, when people are using a VPN to connect into their employers’ networks. When employees are in the office, it seems as though the corporate firewalls function like dams blocking malware-infected machines trying to connect out to the Internet either for command and control or to further compromise other vulnerable machines on the Internet. “However, when you rely on a VPN, it’s like digging a ditch to the side of that dam,” remarked Huttunen.



**Number of unique US organizations and compromise topography mirror trend in Europe.**

In particular, Arctic Security saw that the most prevalent activity associated with the compromised organizations was scanner activity. This means devices that cyber criminals have compromised and intended to employ in identifying vulnerabilities and infecting other machines have been set free in a sense — no longer held at bay by a company’s firewall. “These observations mean that the criminals have control over resources at an increased number of victim organizations,” commented David Chartier, CEO of Arctic Security. “This research helps illustrate the fact that cyber security issues can fall through the cracks of an organization’s layered security approach. This underscores the need to use high quality third-party observations, such as those Team Cymru provides.”

Large enterprises with teams of top tier security analysts have made investments in being able to view their cyber threat exposure from outside their enterprise perimeters. “Many large enterprises have teams of threat analysts with the skills to apply network forensics to the global network,” explained David Monnier, Director of Client Success at Team Cymru. “But most companies lack the staff to analyze global network flows with over 50 other types of data in order to map malicious infrastructures and monitor their security posture from that perspective.”

Despite increases in security investment and advances in internal solutions, such as endpoint detection and response and network monitoring tools, security teams are still overwhelmed by alerts based on imperfect or incomplete data, and they remain resource constrained.

In order to gain that outside-in perspective, companies rely on third-party services firms to help close the gaps left by traditional internal security infrastructure. This allows those resource-constrained organizations to continuously refine their security controls based on what their services partners are seeing in the wild. Unfortunately, the refinements are often correcting simple failures in basic IT operations. “It’s also important to realize that the criminals test their malware and methods against traditional security tools, such as antivirus, explained Chartier. “What we are seeing in our analysis has bypassed all the security controls of these organizations in order to be able to communicate out of those networks. We are witnessing the limitations of traditional internal security tools and processes.”

**Arctic Security Oy**
contact@arcticsecurity.com+358 20 743 0010
Business ID: 2846252-2

Leverage from
the EU
2014–2020

European Union
European Social Fund