Top cyberthreats on enterprise networks

Network traffic monitoring: 2020 data

ptsecurity.com

About the research

The longer that attackers remain undetected by corporate defenders, the deeper they can burrow into infrastructure in order to steal data and make money. Even though attackers can manage to hide their tools from antivirus software, they have a much harder time concealing network traffic, since doing so requires modifying the protocols used to transfer data. Network traffic analysis (NTA) solutions help defenders to see what is going on. NTA can also be called network detection and response (NDR) systems.

IT IS A YEAR-TO-YEAR RESEARCH

We will compare the results for 2019 with those for 2020 and use in-the-field data to describe the biggest threats to the security of corporate networks.

Here we will analyze the results of network monitoring **at 41 companies** that hosted **pilot deployments** of **PT Network Attack Discovery in 2020.**

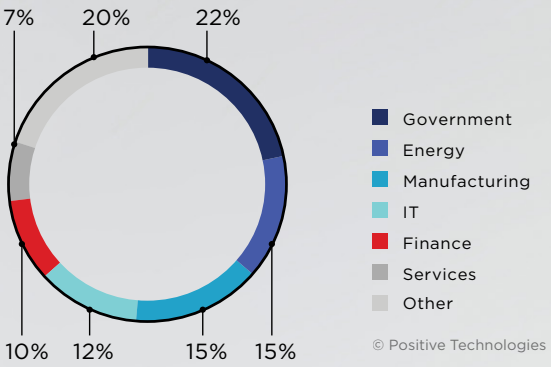

Figure 1. Participant portrait

Only clients who consented to analysis and publication of anonymized network monitoring results have been included in the dataset.

Threat categories

PT NAD detects threats both inside networks and on the perimeter

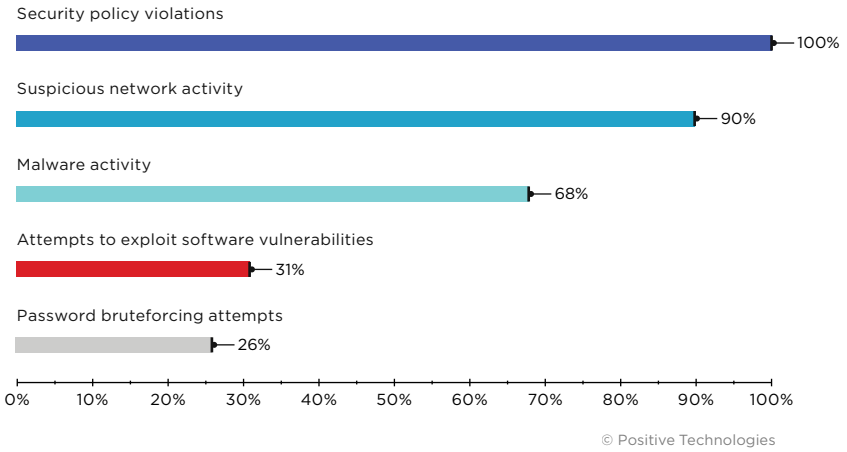

Figure 2. Categories of detected threats (percentage of companies)

Threats were found

on 100%
of corporate infrastructures

on 24%
of perimeters

01 **Security policy violations** were found at every company (100%). Violations included use of remote access software and insecure protocols.

02 **Suspicious network activity**, in keeping with last year, was detected at the vast majority of companies (90%). Traffic concealment, network scanning, and attempts to remotely launch processes all fall under this category.

03 **Malware** is "popular" as well, with activity present at 68 percent of companies.

04 **Software exploitation attempts** took place at one third of companies. Attackers tried to target vulnerabilities both inside the network and on perimeter systems. More than half of attempts involved vulnerability CVE-2017-0144 in the implementation of the SMBv1 protocol. This is the same vulnerability leveraged by the infamous WannaCry ransomware, and for which a patch was released back in 2017. But attackers have kept it in their arsenals as they search for computers that have not been updated in the last 3.5 years. Attempts to exploit CVE-2017-0144 were a frequent occurrence in 2019 as well, affecting one fifth of companies.

05 **Password bruteforcing attempts (26%)** were also picked up by network traffic analysis. At one company, for example, attackers tried to bruteforce the password of a web-accessible database management system. If successful, the attackers would have been able to access the website database, including user credentials.

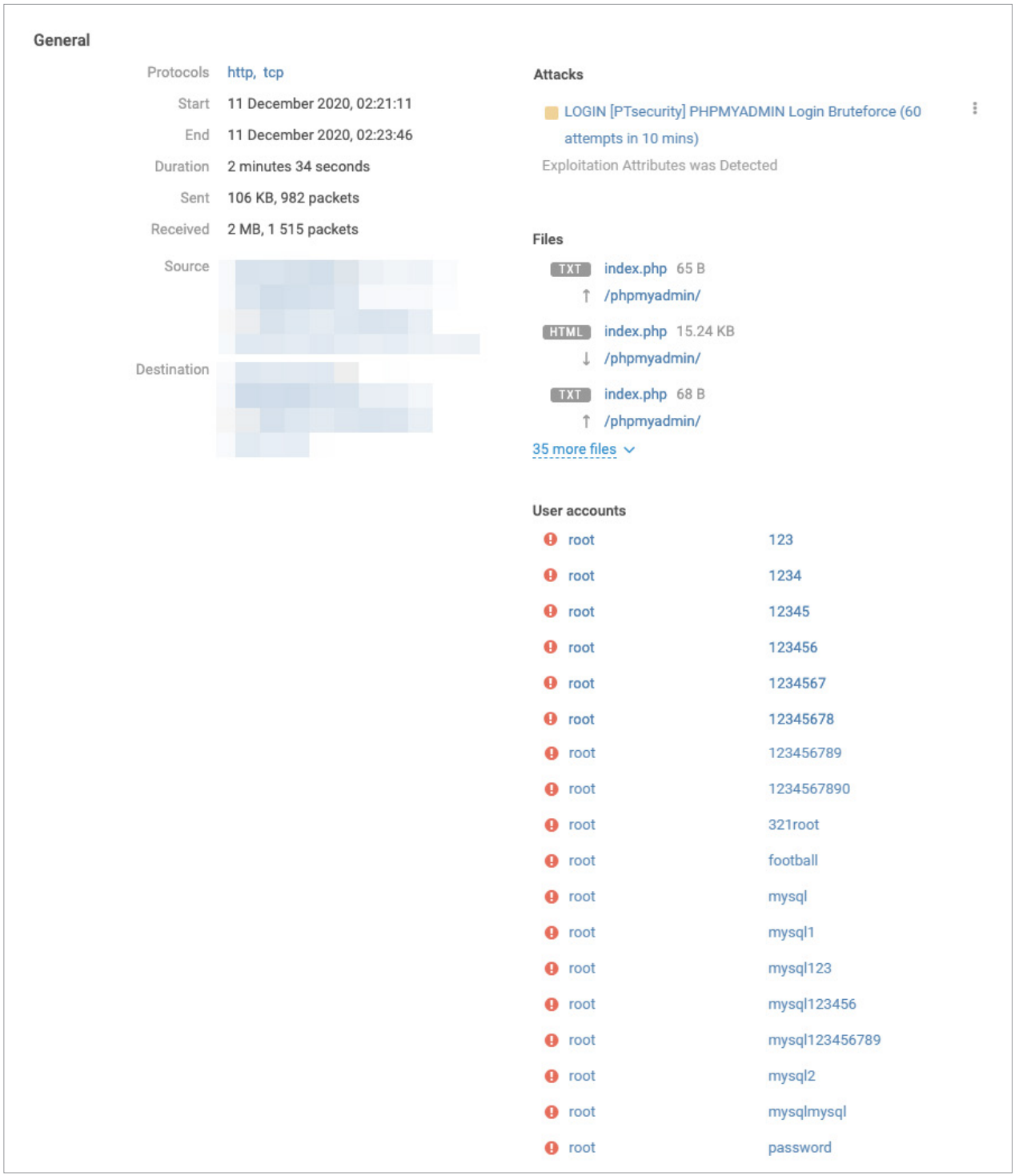

Figure 3. Attempted bruteforcing of credentials

Let's take a closer look at the most frequently encountered threat categories: **violations of security policies, suspicious network activity, and malware activity.**

01 Policy violations detected at 100% of companies

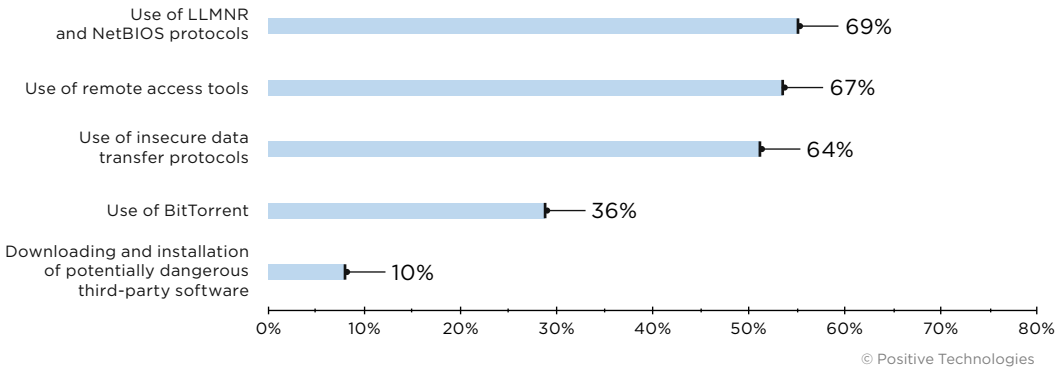

Figure 4. Five most common policy violations (percentage of companies)

Use of remote access software was one of the most frequent security policy violations. Many companies used TeamViewer (59%) and Ammyy Admin (21%). Other active software included LightManager, Remote Manipulator System (RMS), Dameware Remote Control (DWRC), and AnyDesk.

Almost half of companies
that use remote access have multiple programs for it installed. At one government client, five different programs were detected: Ammyy Admin, RMS, AeroAdmin, LiteManager, and TeamViewer.

At 6 out of 7
manufacturing companies, remote access software was used in violation of security policies.

Even popular remote access software can contain critical vulnerabilities. One such vulnerability, CVE-2019-11769, allows an attacker to grab TeamViewer credentials from process memory in cleartext. Remote access software also offers attackers a way to access infrastructure without being noticed. That's why, for companies that cannot do away with remote access entirely, we recommend using just one program for remote access and keeping it fully up to date.

The out-of-date LLMNR and NetBIOS protocols are still used at 69 percent of companies. This configuration flaw can be used to intercept NetNTLMv2 challenge–response values for bruteforcing passwords.

02 RDP connections are growing, but how legitimate are they?

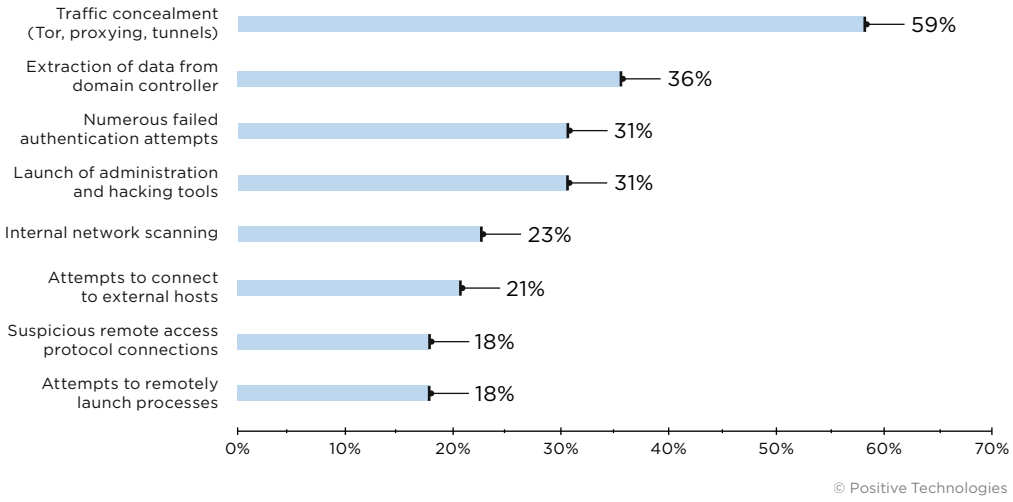

Figure 5. Suspicious network activity (percentage of companies)

At 4 out of 5

IT compaines traffic concealment (Tor, proxying, tunnels) was detected

Work from home has certainly impacted network activity, with significant growth in RDP for accessing internal corporate networks: RDP connection prevalence, from just 3 percent of companies in 2019, jumped to 18 percent in 2020. Clearly, such connections must be carefully monitored.

At one manufacturing company, PT NAD detected an RDP connection to external cloud storage. A total of 23 GB of data had been uploaded over RDP and HTTPS. This may have been a case of attackers applying MITRE ATT&CK technique T1071 (Application Layer Protocol). In essence, attackers or malware stealthily exfiltrate stolen data to servers they control with the help of common application-layer protocols.

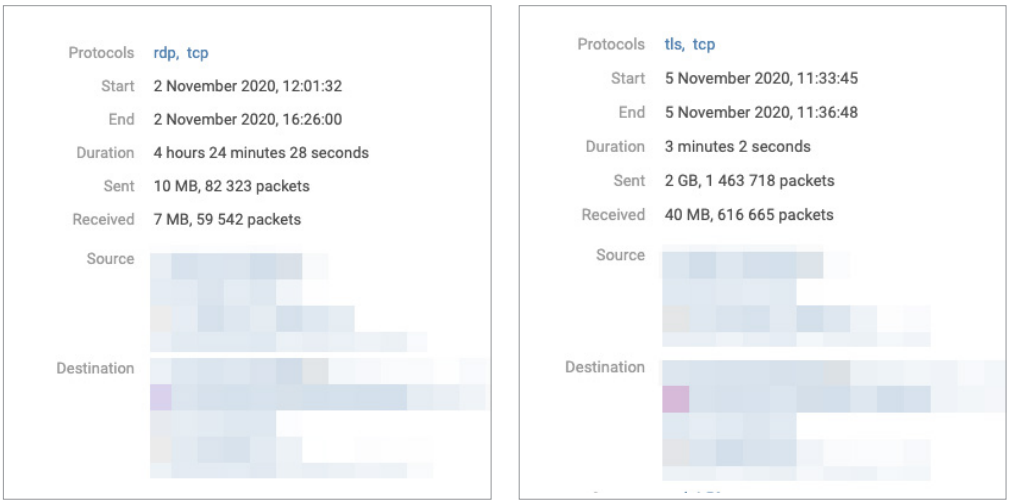

Figure 6. Suspicious RDP and HTTPS connections

At half of manufacturing companies, we detected data flows from the domain controller. While such activity can be legitimate, exports of domain groups or the list of domain admins can also indicate ongoing reconnaissance as part of an attack.

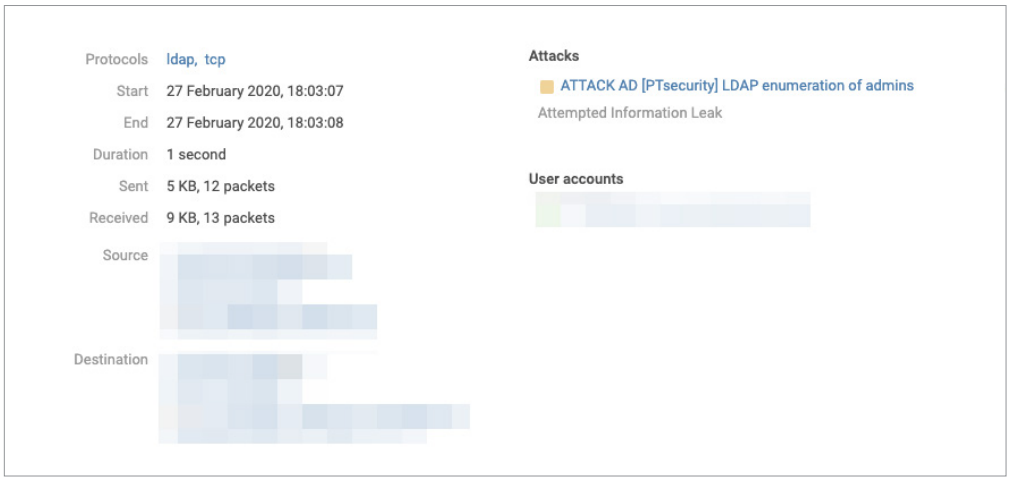

Figure 7. Attempt to obtain information about administrator accounts via LDAP

03 Malware detected at every government and manufacturing company tested

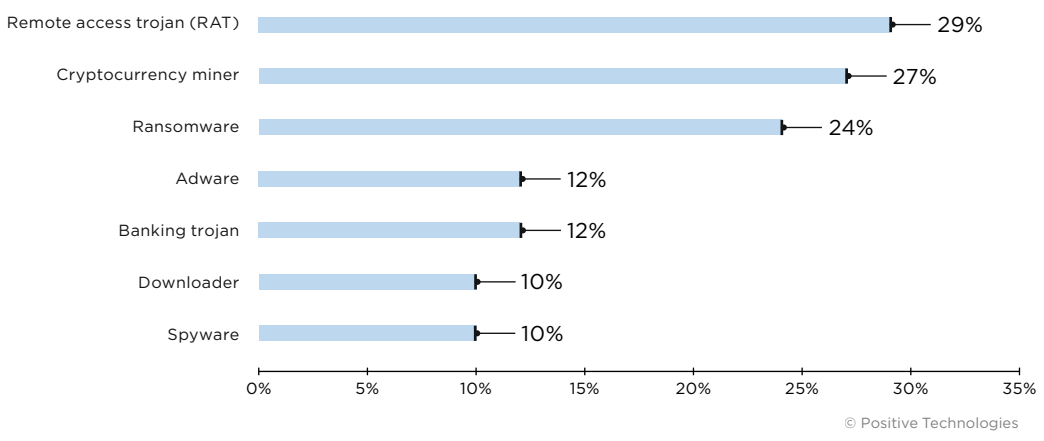

Figure 8. Five most common types of malware found (percentage of companies)

At one fourth of companies, we detected attempts to connect to sinkholed domains (these are domain addresses that have been previously implicated in malicious campaigns; any connection attempts are redirected to special sinkhole servers to block malware from contacting C2 servers). Remote process launching was detected at one out of five companies. Such network activity can be indicative of malware.

In pilot projects for monitoring network activity and detecting advanced persistent threats in 2020, we encountered a total of 36 families of malware. These included WannaCry ransomware as well as the RTM, Ursnif, and Dridex banking trojans.

AgentTesla spyware was detected at three companies. In spring 2020, AgentTesla was encountered in phishing campaigns that took advantage of COVID-19 concerns. The malware was modified to steal credentials for email accounts from Microsoft Outlook as well as Wi-Fi passwords.

One fourth of companies had cryptocurrency miners on their networks. Generally speaking, in these cases PT NAD detected requests to resolve domain names associated with mining pools, such as antpool.com, supportxmr.com, minexmr.com, nanopool.org, xmrpool.eu, monerohash.com, and io.litecoinpool.org. Attackers can install miners either at the same time as their primary malware or after achieving their main objective, such as data theft. Since miners can consume up to 80 percent of available CPU capacity, performance of company systems may slow to a crawl.

At 68%

of tested companies malware activity was detected

Detection of any malware on infrastructure is cause for a thorough investigation. Malware can be an indicator of serious issues in a company's security stance.

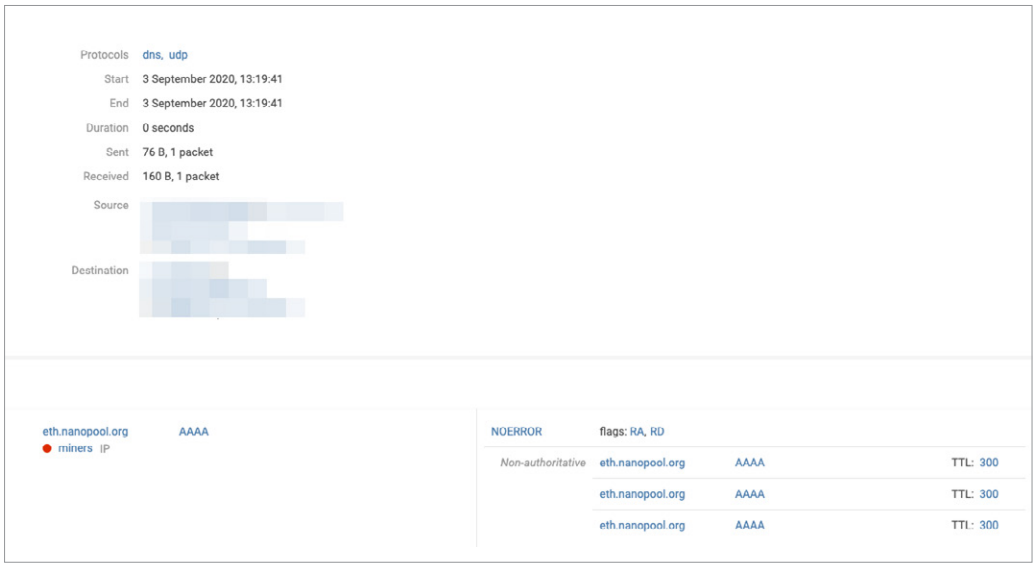

Figure 9. Attempt to resolve the domain name of a known mining pool

NDR/NTA systems are increasingly being installed inside corporate infrastructure, instead of for detecting external attacks

Conclusion

Companies are taking a more serious approach to selecting, piloting, and deploying protection solutions. In our experience, NDR/NTA systems are increasingly being installed inside corporate infrastructure, instead of for detecting external attacks. This approach is more involved, due to requiring a good understanding of internal infrastructure and network topology. However, it also has a significant upside: detection of suspicious activity within internal networks.

Overall, the results of network traffic analysis for 2020 are similar to the year prior:

- Every company had violations of security policies, especially use of remote access software and insecure or obsolete data transfer protocols.
- As work from home arrangements increased in popularity, so too did RDP connections. These connections need to be carefully monitored: in 2020, the number of attacks on remote access protocols more than tripled.
- Almost every company harbored suspicious network activity such as traffic concealment or suspicious connections to external hosts.

Deploying NTA enables catching suspicious connections before it's too late, and even looking back at a host's network history to check for previous attempts.

For example, even if an attack has already occurred and there were no detection rules or indicators of compromise known at the time, some may have appeared more recently. This is why traffic should be analyzed in real time and also retrospectively as new information becomes available. By retaining a copy of traffic and analyzing it at a later date, companies can perform detailed investigations and retrace the actions of an attacker even for events in the past.

NAD2020_A4.ENG.0001.03.MAR.18.2021