# Top cybersecurity threats on enterprise networks

Network traffic analysis: field findings

ptsecurity.com

# Contents

# What is Network Traffic Analysis

The IT infrastructure of large modern companies generates huge amounts of network traffic every day. Keeping track of vulnerable spots in communication between devices is getting even more difficult as infrastructure grows larger and new technologies appear. Meanwhile, cybercriminals have a whole range of techniques for hiding their presence on compromised infrastructure and masking their malicious traffic as legitimate. Information about connection addresses, network ports, and protocols is no longer sufficient for timely threat detection and response. What is needed is advanced traffic analysis, with protocols analyzed all the way to the application level (L7). This is what Network Traffic Analysis (NTA) solutions are designed to do.

NTA systems combine machine learning algorithms, behavioral analysis, rule-based detection, and threat-hunting features. These methods enable detecting suspicious network activity, malware activity, attempted exploitation of vulnerabilities both on the perimeter and inside the network, non-compliance with information security policies, and other threats. Gartner analysts state that a number of companies use NTA solutions as part of their security operations centers (SOCs).

# About this research

In 2018, Positive Technologies released a new NTA solution called PT Network Attack Discovery (PT NAD). This report summarizes the results of network activity monitoring on the infrastructure of 36 companies where PT NAD was deployed as a pilot project. The average duration of each pilot project was one month. Findings here are taken from projects completed in 2019 at large companies (1,000+ employees) in key sectors in Eastern European countries. The dataset consists only of pilot projects for which clients consented to use of network activity monitoring results and publication of depersonalized data.

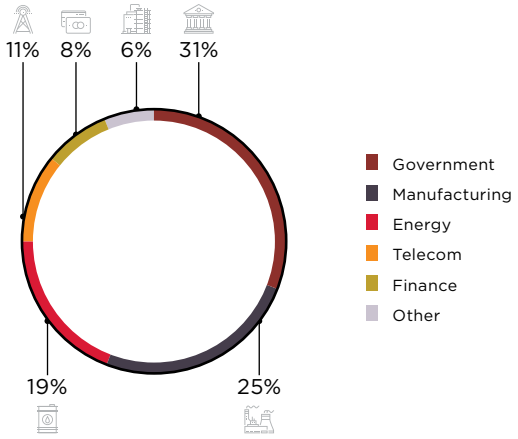



Figure 1. Client snapshot

# What lies inside the network

For illustration purposes, we divided all threats found on enterprise networks into several categories. Suspicious network activity was detected on the infrastructure of 97 percent of companies. Advanced network traffic analysis revealed non-compliance with security policies on the infrastructure of 94 percent of companies. Malware activity was detected at 81 percent of companies. Let us look closely at the most common threats in these categories, in order to understand the dangers they contain.

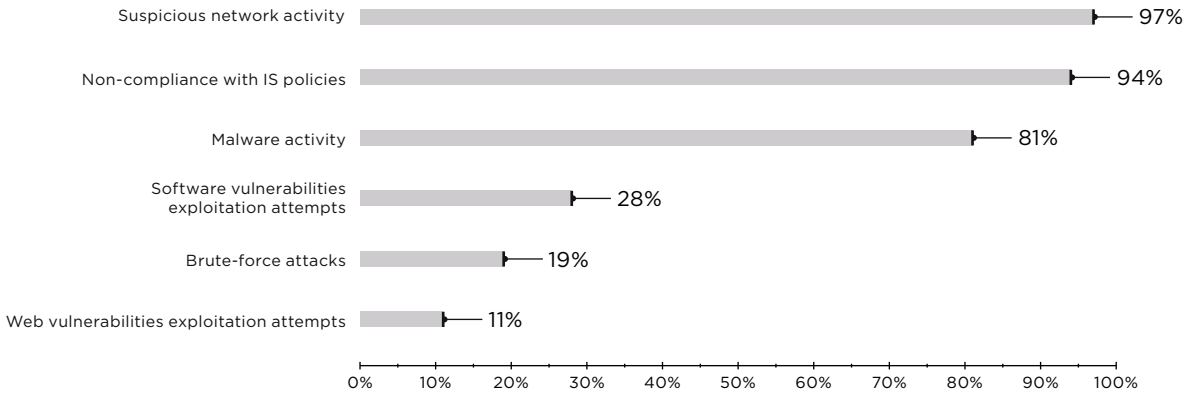



Figure 2. Categories of detected threats (percentage of companies)

# Suspicious network activity

Which traffic is considered suspicious? Examples include VPNs, proxies, and Tor connections. These were found at 64 percent of companies.

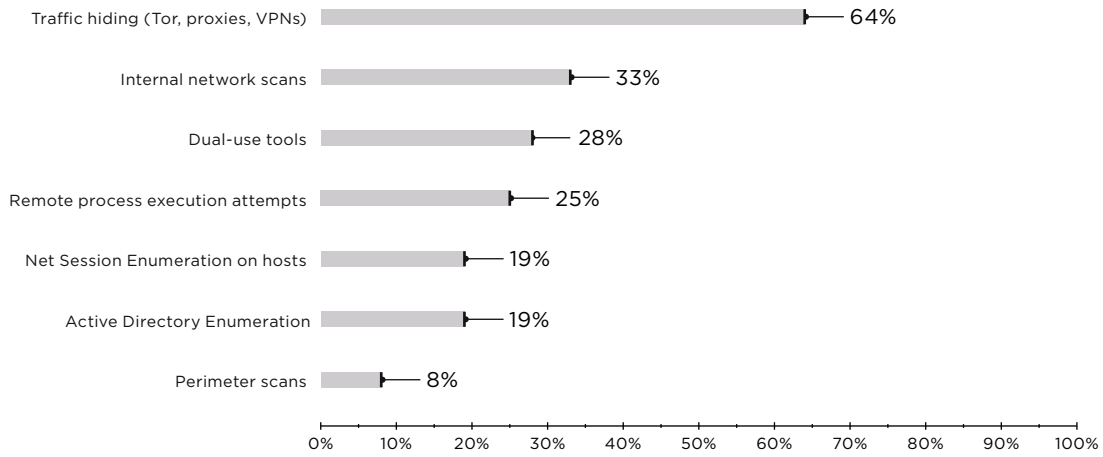
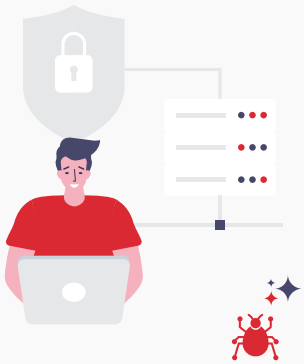



Figure 3. Suspicious network activity (percentage of companies)



## What are the dangers of Tor, VPNs, and proxies?

When employees connect to Tor, access proxy servers, or use a VPN to bypass site blocking, malefactors can use the same technologies to communicate with command-and-control (C2) servers. For instance, the ZxShell backdoor of the APT41 group can establish proxy connections via SOCKS and HTTP. Professional hackers can also encrypt traffic between malware and C2 servers. NTA solutions can detect anomalies in SSL/TLS traffic.

Suspicious network activity also includes actions indicative of attacker intelligence gathering and lateral movement. Such actions include network scans, multiple failed attempts to connect to hosts, and traces of collecting intelligence on active network sessions on a specific host or entire domain.

**22%**

**of companies** had signs of PsExec use

At 28 percent of companies, we discovered activity of certain tools and utilities that may suggest a compromise. Why do we say "may suggest" and how can we prove that hypothesis? The current trend is toward so-called living off the land attacks. Such attacks use mechanisms built in to the OS, as well as trusted programs, for remote command execution on hosts. On Windows-based infrastructure these may include PowerShell, WMI, and Sysinternals. PsExec, for one, is a utility equally appreciated by IT administrators and black hats.

It is hard to tell in real time whether an action is performed by attackers using legitimate tools or by a system administrator. No security tool can do so with absolute accuracy. That is why attackers can use legitimate tools and remain unnoticed for a very long time.

One of the ways of detecting a living off the land attack is network traffic storage and analysis. Traffic contains information about seemingly innocent actions. This is important for retrospective analysis during incident investigation, when the specialist needs to reconstruct the timeline of network events and walk back the attack chain. Such works are generally outside of our pilot projects, so when suspicious network activity is detected, we consider it only a potential compromise. There are exceptions, of course. At one company where the pilot project revealed traces of an APT group's presence, network traffic analysis detected evidence of use by attackers of legitimate Sysinternals tools, specifically PsExec and ProcDump. Timely detection enabled us to block the attackers' actions.

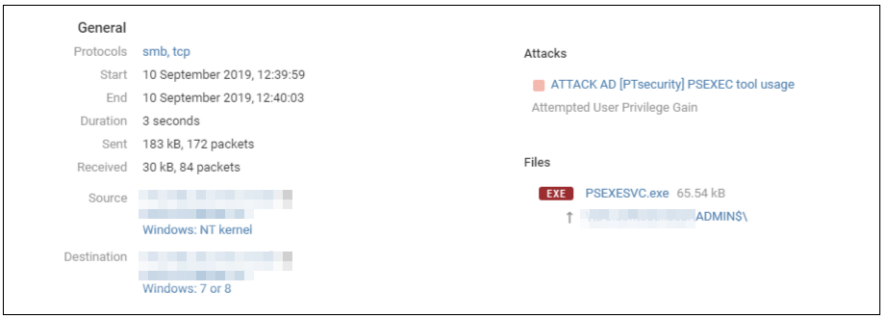



Figure 4. Remote Command Execution with PsExec

# Malware activity

Certain anomalies in traffic can indicate malware infection with great probability. At 39 percent of companies, we detected attempts by servers and workstations to connect to sinkholed domains.


## What is a sinkholed domain?

It's a domain name that has been involved in malware campaigns. Connections to such addresses are redirected to special sinkhole servers, preventing malware from connecting to the actual C2 servers. Requests attempting to access sinkholed domains are a sure sign of malware infection.

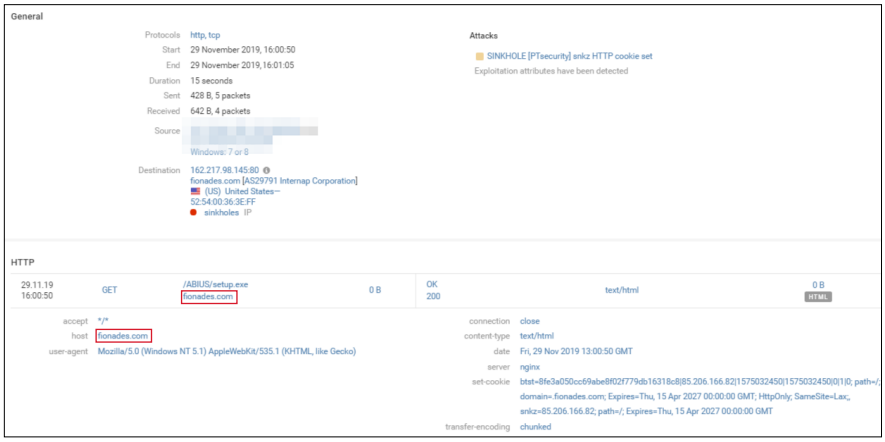



Figure 5. Attempts to resolve a sinkholed domain name

Requests to sinkholed domains can indicate threats of various severity, from run-of-the-mill spam bots to a complex targeted attack. In one of the pilot projects we checked the customer's corporate network and detected requests to three sinkholed domains. Two of those domains were involved in APT attacks by the Sofacy group (APT28).

Reputation lists are databases of addresses involved in malware campaigns. These databases are updated regularly, and then imported into security tools to block malicious activity. But attackers have figured out how to bypass security that relies on indicators of compromise. Advanced malware can generate domain names for C2 servers dynamically with special domain generation algorithms (DGAs). At several companies, PT NAD detected requests to automatically generated addresses.


Figure 6. Examples of DGA domains

Multiple attempts to connect to external servers via port 445/TCP (SMB) are another example of suspicious network activity indicative of malware infection. This is consistent with the presence of WannaCry ransomware or other malware distributed in a similar manner. There are other indicators, such as requests to killswitch addresses, related to WannaCry. But the most common malware found on infrastructure was miners (found at 55% of infected companies) and adware (28%). 47 percent of companies were infected with several different types of malware.

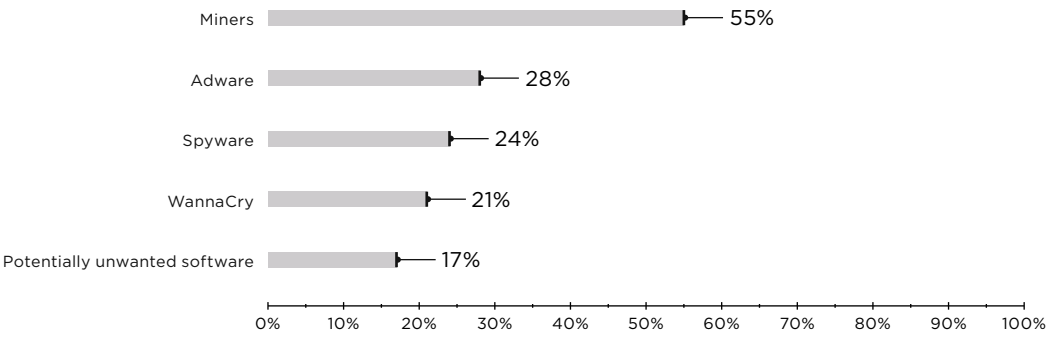



Figure 7. Top 5 malware types (percentage of infected companies)

It would be foolish to think that the worst a miner can do is cause large electricity bills, or that the worst you can expect from adware is annoying pop-ups. If your computer is infected with any malware, you need to identify the source of the threat as soon as possible. Your computer could have been infected through a breach of the infrastructure, and attackers can use such breaches to deal more damage than one might initially think. At one company, we found a host on the perimeter with open port 445/TCP (SMB), as well as multiple attempts to exploit vulnerability MS17-010 on that host.

# Non-compliance with IS policies

Security policies at many organizations do not allow employees to visit questionable sites, download torrents, install chat programs, or use remote access utilities. These measures are there to maintain an acceptable security level, but quite often employees ignore them. The reasons for this are varied but we will not dwell on them here. Suffice it to say that non-compliance with information security policies was found at 94 percent of companies. This calls for a reminder of the consequences of poor "network hygiene."

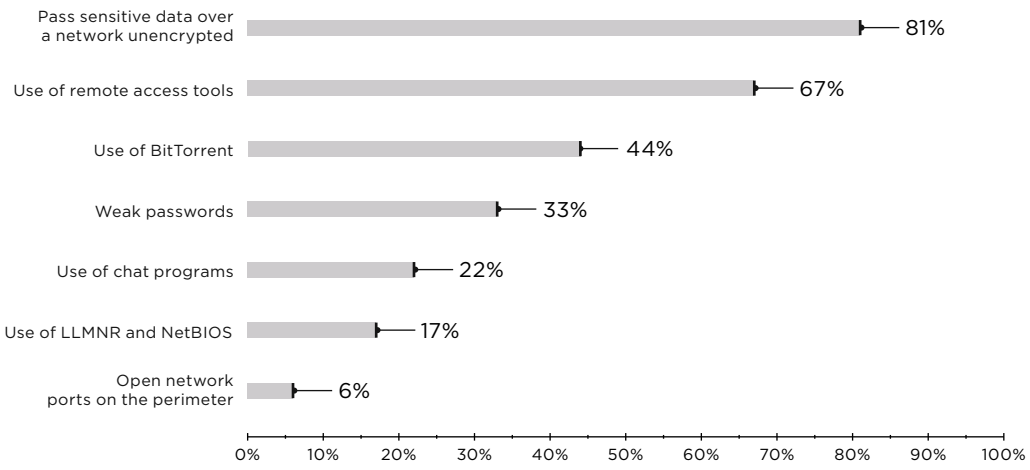



Figure 8. Top 7 types of non-compliance with IS policies (percentage of companies)

## Insecure protocols inside the network: dangerous or not

At 81 percent of companies, sensitive data is transmitted in cleartext. This means that anyone on the corporate network, including a potential attacker, can intercept traffic and search it for sensitive information such as usernames and passwords. Another problem often found, along with unsecured protocols, is dictionary passwords.

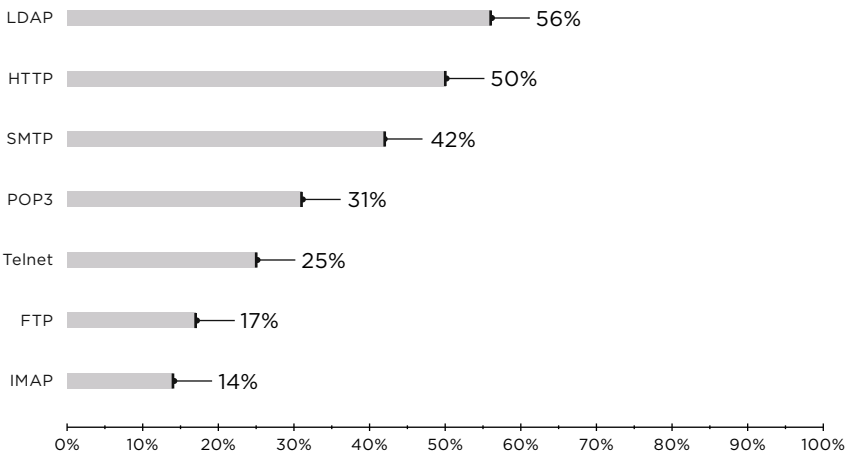



Figure 9. Pass sensitive data over a network unencrypted (percentage of companies)

We found that at 56 percent of companies, unencrypted credentials are transmitted via LDAP. This protocol is used by directory services. Administrators use them for centralized administration and for managing access to network resources. If attackers can intercept domain credentials in insecure LDAP traffic, they can use these credentials to move deeper into the network.

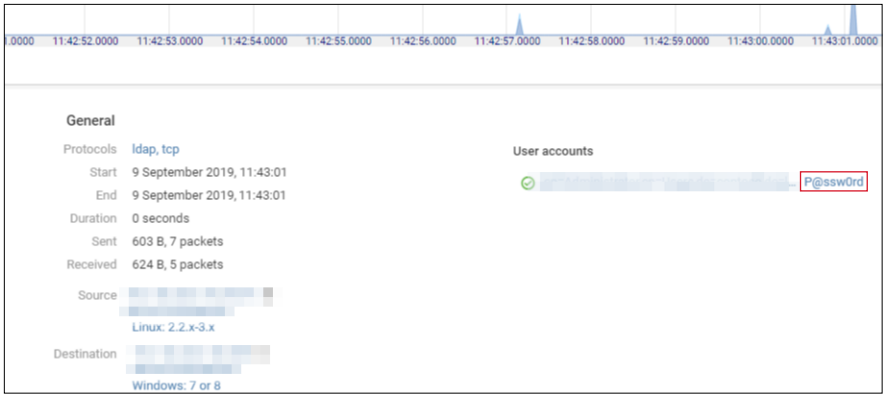



Figure 10. Transmission of cleartext credentials via LDAP

One out of two companies still uses the insecure HTTP protocol for accessing the web interfaces of internal services. For instance, two companies transmitted usernames and passwords for the Zabbix monitoring system in cleartext in the request body. What threats come with this authentication choice? One, compromised credentials can help in obtaining information about models and versions of software and hardware used on the infrastructure, making it easier for malefactors to gather intelligence inside the network. Two, if the attackers pilfer Zabbix administrator credentials, they can execute OS commands on the server and use the server for further attacks.

Another example of insecure data transfer via HTTP is Basic authentication. With Basic authentication, credentials are transferred in the request header in Base64 encoding. If attackers read packets with authentication requests, they can find the header and decode the password. This threat was found at 33 percent of companies.

Unencrypted email traffic is also a threat of concern. 42 percent of companies had not set up secure connections (TLS) for outgoing email messages. If attackers gain access to the company's external network traffic, they can read messages sent by employees via the Internet. The ISP has access to the company's external traffic, of course. The ISP, too, may fall victim to a cyberattack. Alternately, attackers can get their hands on unencrypted messages from the ISP's equipment with help from an insider.

## Recommendations

Use secure protocols such as HTTPS, SLDAP, Kerberos, SFTP, FTPS, and SSH. Set up mail clients and servers to use TLS. Do not use weak passwords or default passwords. Review your password policy to make sure that passwords are strong enough. Make sure that the policy is followed by employees.

**58%**

**of companies**
use TeamViewer
for remote access

## Remote access tools: convenience vs. risk

Another threat comes from remote access tools. 67 percent of companies use RAdmin, TeamViewer, Ammyy Admin, and other similar tools. This is certainly convenient for employees working from home. But what are the risks? The employee's personal computer can be hacked and then attackers can connect to the corporate network via remote access.

Remote access is also useful for IT contractors. We recommend avoiding such use, however. APT groups today abuse the trusting relationship between victims and the victims' partners, agents, or contractors. Remember that abnormally long connection times or connections outside of normal business hours may be signs of compromise.

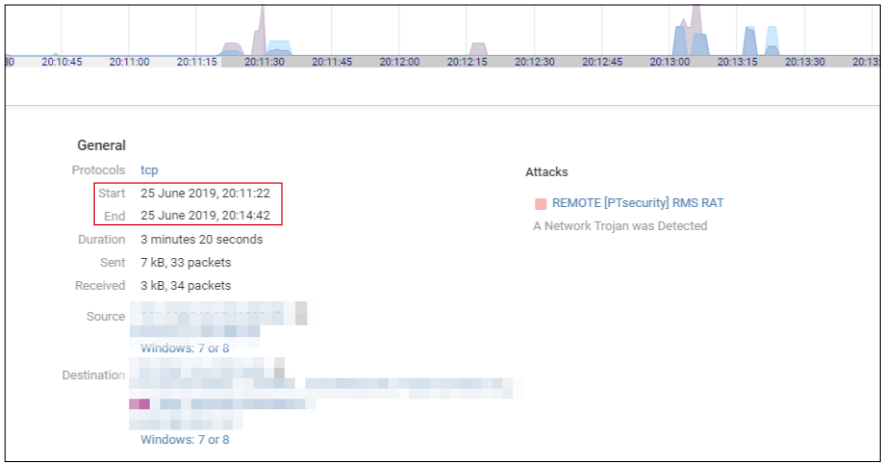



Figure 11. Suspicious connection via RMS outside of business hours

Broadly speaking, it does not really matter how and for what purpose the company uses remote access tools. What matters is, if the attackers get inside the infrastructure, they can use remote access tools to move inside the network unnoticed by security tools, because they will act posing as a trusted entity using an approved access method.

## Recommendations

If you absolutely must use remote access tools, use only one. Restrict access rights of local users and create a software whitelist with AppLocker.

## Torrents: block or allow?

Our pilot projects demonstrated that at 44 percent of companies, employees use peer-to-peer networks for data transfer, such as downloading torrents. This places an extra burden on the network and consumes bandwidth. But there's another risk. Malware may be lurking on torrent trackers, posing as various software, movies, and other files. A tempting torrent may lead to a ransomware attack or deliver the malware of professional cybercriminals. For instance, torrents were used to distribute STOP ransomware and the APT37 group weaponized a YouTube video downloader app with the KARAE backdoor and distributed it on torrent websites.



## Recommendations

Introduce a company-wide ban on BitTorrent data transfers. Implement a whitelist policy with AppLocker.

Cybersecurity must be more than just the perimeter and traditional security tools. Our research indicates that 92 percent of threats are detected when the enemy is already inside.

Cybergroups breach the security on the perimeter of their targets. This is evident from the growing percentage of successful targeted attacks. This is a good reason to shift attention from prevention of attacks on the perimeter to timely detection and response inside the network. However, it is hard to detect a well-planned cyberattack, especially when it is extended over time. Attackers are no longer hindered by antivirus software. They constantly modify source code, use bodyless malware, and exploit zero-day vulnerabilities. Dynamic analysis is no cure-all, either. Attackers have learned to bypass the virtualization technologies typically used in sandboxes. And we cannot rule out the possibility that attackers can get by without any malware at all, just using the tools permitted by the target's security policies.

However, attackers leave traces in network traffic, so it's up to cybersecurity specialists to find those traces. Our pilot projects have demonstrated that NTA solutions are effective at detecting threats on the internal network, ranging from non-compliance with IS policies to complex targeted attacks.

# PT Network Attack Discovery

PT Network Attack Discovery (PT NAD) is a deep network traffic analysis system used to detect attacks on the perimeter and within the network.

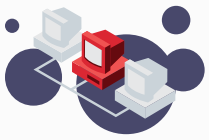
## Main benefits of PT NAD

01

**Provides network visibility.** PT NAD identifies over 70 protocols and parses the 30 most common ones up to and including the OSI L7 level. This provides a full picture of what is going on in the infrastructure, helping to identify security flaws that can weaken security and enable attack progression.

02

**Detects threats on the perimeter and inside.** PT NAD draws on indicators of compromise, rules-based detection, machine learning, and retrospective analysis. Rules and IoC for PT NAD are updated twice a week by an in-house research team. Positive Technologies is a MAPP member. We receive information about zero-day vulnerabilities in Microsoft's products. That's why PT NAD's customers get protection faster.



03

**Helps in detection of targeted attacks.** PT NAD uses heuristic methods, behavioral analysis, and can detect anomalies in encrypted traffic. As soon as an update to the knowledge base appears, traffic can be re-analyzed. Such retrospective analysis detects new types of infrastructure threats not detected previously.

04

**Effective for investigations.** PT NAD stores records of captured traffic, as well as 1,200 parameters of network interactions. The security analyst can quickly learn what happened before a suspicious security event, what servers the compromised host communicated with, and how the attack began.




ptsecurity.com
info@ptsecurity.com