VECTRA

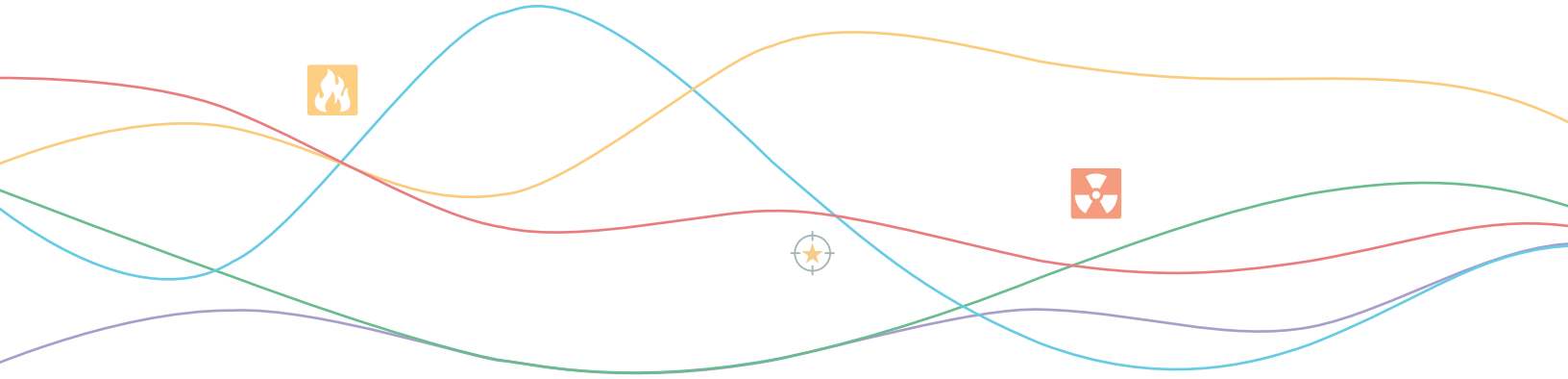
I am artificial intelligence.
The driving force behind the hunt for cyberattackers.
I am Cognito.

The hidden threat of cyberattacks in the energy and utilities industry

2018 Spotlight Report

VECTRA

TABLE OF CONTENTS



Since at least March 2016, Russian government cyber actors targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.

An analysis by the U.S. Department of Homeland Security (DHS) and FBI provides insight into the attacker behaviors related to this malicious activity. The report, *Dragonfly: Western energy sector targeted by sophisticated attack group*, released by Symantec on Sept. 6, 2017, provides additional information about this ongoing cyber campaign.

Unfortunately, this is not new. But it highlights an important distinction in attacks that target the energy and utilities industry.

There is a difference between attacks that probe IT networks for information and access about critical infrastructure *versus* attacks against the industrial control system (ICS) on which the critical infrastructure operates. The two are interconnected, but the targeted assets are different.

Cybercriminals have been testing and mapping-out attacks against energy and utilities networks for years. These slow, quiet reconnaissance missions involve observing operator behaviors and building a unique plan of attack. The attack that shut down the Ukraine power grid in 2015 was reportedly planned many months in advance by highly skilled and sophisticated cybercriminals.

Although the ICS is in the crosshairs, most attacks against the energy and utilities industry occur and succeed inside the enterprise IT network – not in the critical infrastructure.

This underscores the importance of identifying hidden attackers inside IT networks before they cause damage to the ICS and steal critical infrastructure blueprints. This spotlight report focuses on those specific cyberattacker behaviors as they relate to the latest attack campaigns used to steal vital ICS information.

Analysis and lifecycle of an attack on critical infrastructure

A U.S. government alert known as TA18-074A, released by the DHS computer emergency readiness team in March 2018, outlines Russian government cyber activity targeting energy and other critical infrastructure sectors.

The attack campaign detailed in TA18-074A involves two categories of victims: Staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks. Threat actors used the staging targets' networks as pivot points and malware repositories when targeting their final intended victims.

The National Cybersecurity & Communications Integration Center (NCCIC), which is part of the DHS, and the FBI determined that the objective of this attack was to compromise organizational networks.

Command and control

To carry out this attack, threat actors created web shells on the intended targets' publicly accessible email and web servers. They used three different file names – global.aspx, autodiscover.aspx and index.aspx – for two different web shells. The difference between the two groups was the *public-string password* field.

The DHS and FBI determined that threat actors leveraged remote access services and infrastructure such as VPN, Remote Desktop Protocol (RDP) and Outlook Web Access (OWA). Threat actors used the infrastructure of staging targets to connect to several intended targets. *This command-and-control behavior is known as external remote access*.

Internal reconnaissance

Upon gaining access to the intended victims, the threat actors launched reconnaissance operations inside the network. DHS observed the threat actors identifying and browsing file servers within the intended victim's network. *These reconnaissance behaviors are known as file-share enumeration and RDP recon*.

Lateral movement

Once inside the targeted network, threat actors used privileged credentials to access the victim's domain controller, typically using RDP. Once on the domain controller, threat actors used *dc.bat* and *dit.bat* batch scripts to enumerate host devices, users and additional information about the environment. *This type of lateral movement behavior is known as suspicious admin*.

In at least two instances, threat actors used batch scripts labeled *pss.bat* and *psc.bat* to run the PsExec tool. In addition, threat actors changed the name of the PsExec tool to *ps.exe*. *This type of lateral movement behavior is known as suspicious remote execution*.

Targeting the ICS and SCADA Infrastructure

In multiple instances, threat actors accessed workstations and servers on a corporate network that contained data output from the ICS inside energy generation facilities. *This involved suspicious admin and suspicious Kerberos account behaviors*.

The threat actors accessed files pertaining to ICS or supervisory control and data acquisition (SCADA) systems. Based on a DHS analysis of existing compromises, these file names included ICS vendor labels and ICS reference documents pertaining to the organization, such as *SCADA WIRING DIAGRAM.pdf and SCADA PANEL LAYOUTS.xlsx*. *These types of actions are known as data smuggler behaviors*.

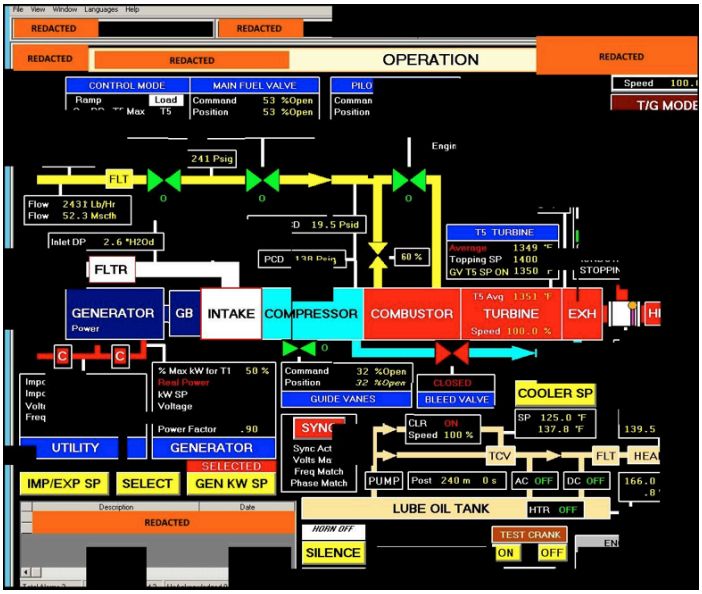


Figure 1: In the federal alert known as TA18-074A, the DHS reconstructed samples of data extracted from energy and utilities organizations by attackers

Analysis of cyberattacker behaviors in the energy and utilities industry

The information in this spotlight report is based on observations and data from the 2018 Black Hat Edition of the Attacker Behavior Industry Report from Vectra®. The report reveals attacker behaviors and trends in networks from over 250 opt-in customers in manufacturing and eight other industries.

From January-June 2018, the Cognito™ cyberattack-detection and threat-hunting platform from Vectra monitored network traffic and collected rich metadata from more than 4 million devices and workloads from customer cloud, data center and enterprise environments.

The analysis of this metadata provides a better understanding about attacker behaviors and trends as well as business risks, enabling Vectra energy and utilities customers to avoid catastrophic data breaches.

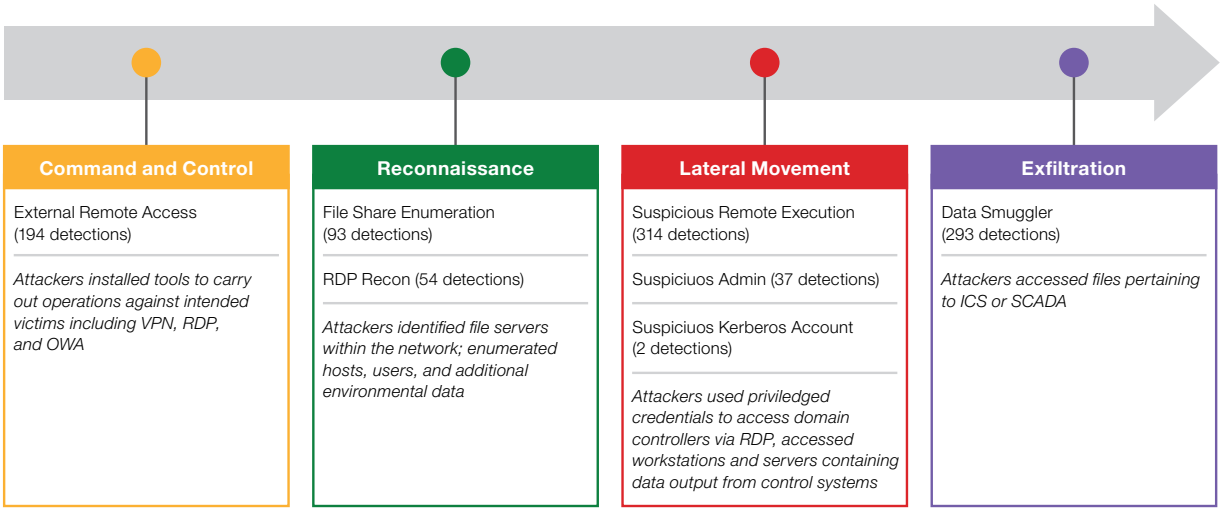


Figure 2: Monthly number of attacker behaviors in the energy and utilities industry per 10,000 devices and workloads

The Cognito platform observed that cyberattackers used the same types of threat behaviors to spy, spread, and steal data from energy and utilities enterprise networks. Every industry has a profile of network and user behaviors specific to their industry because of their business model, applications and processes. These behavior profiles allow attackers to hide, making it difficult for anomaly detection to succeed because their behaviors blend in with traffic from legitimate users.

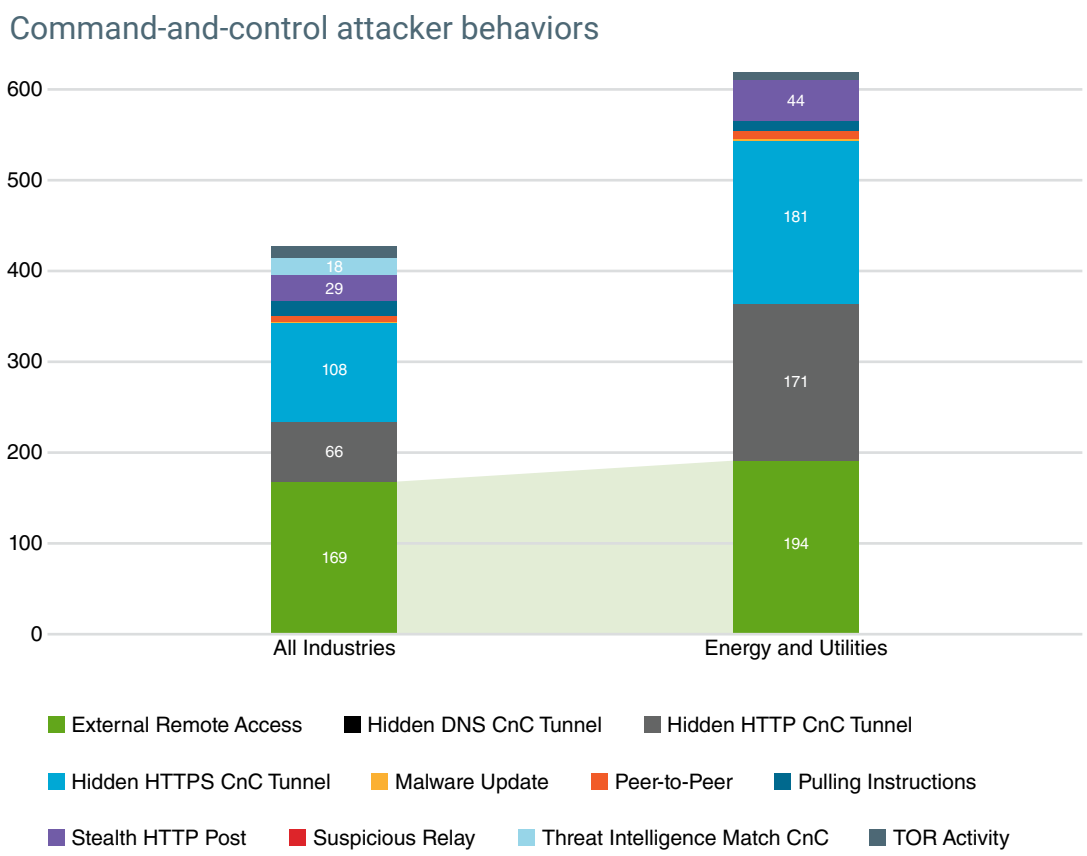


Figure 3: Command-and-control attacker behaviors in the energy and utilities industry per 10,000 host devices

Every cyberattack begins with some form of command and control, and one of the most dangerous forms is external remote access. The Cognito platform detected 194 command-and-control attack behaviors for every 10,000 host devices inside energy and utilities networks, as shown in Figure 3.

With external remote access, attackers directly control host devices rather than using an automated form of command and control. External remote access behaviors can involve internal host devices connecting to an external server. In this case, the traffic pattern is inverse from normal client-to-server traffic. Clients receive instructions from the server and a human on the outside controls the exchange.

Energy and utilities organizations use forms of remote access technology to improve productivity and it can be a legitimate command-and-control behavior. However, the presence of remote network access traffic introduces a risk because it enables attackers to blend in while performing the same types of external remote access for nefarious deeds. This is especially true when attackers leverage commonly-used remote access tools like FortiClient VPN.

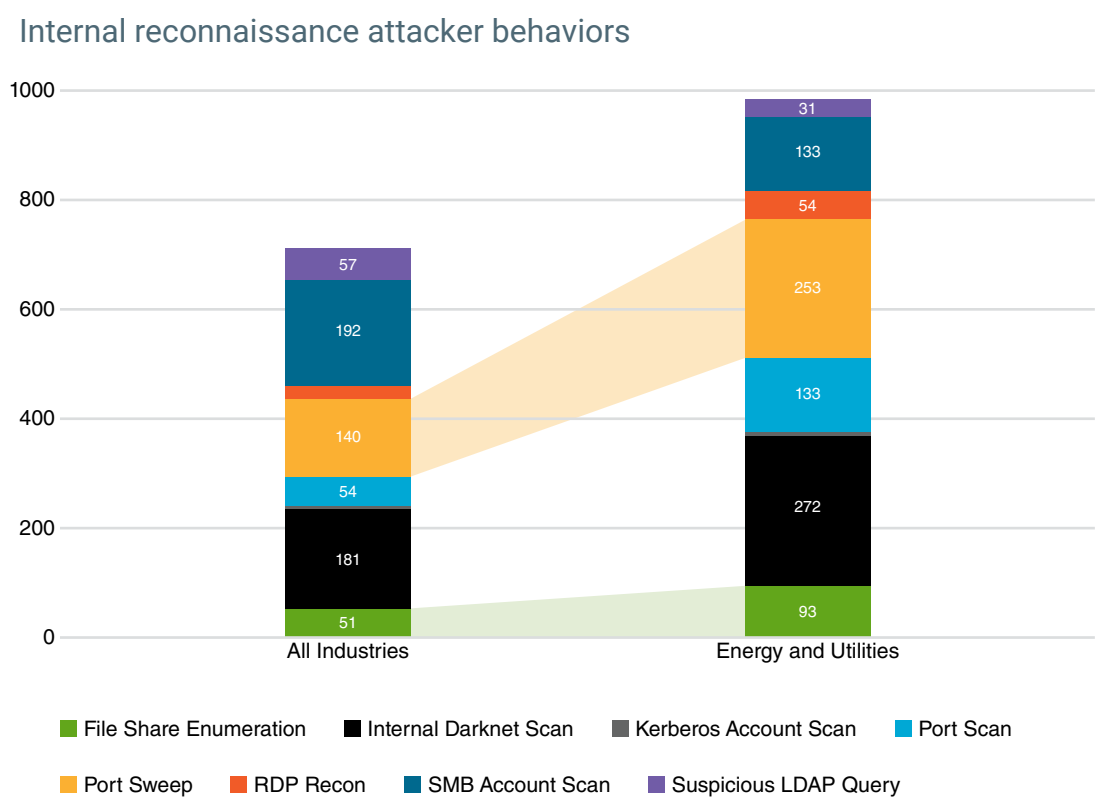


Figure 4: Reconnaissance attacker behaviors in the energy and utilities industry per 10,000 host devices

Reconnaissance inside a network is a precursor to the more risky and damaging stages of active attacks that ultimately exposes an organization to the substantial risk of data acquisition and exfiltration.

The two most prevalent reconnaissance behaviors in the DHS report are file-share enumeration and RDP recon activity. As shown in Figure 4, the Cognito platform detected 93 file-share enumeration attempts in energy and utilities per 10,000 host devices and workloads. RDP recon activity occurred 54 times per 10,000 host devices and workloads.

File-share enumeration behaviors occur when a host device accesses inordinately more file-shares than normal. Enumeration might indicate a host device is accessing many file-shares as a user attempts to find a file or directory. However, enumerating file-shares on a network is also an effective way for attackers to find data to exfiltrate or data that helps further the attack.

In conjunction with file-share enumeration, a scan via RDP is an effective way for an attacker to determine the accounts available within an organization's network and the RDP servers that accept logins via the accounts. File-share enumeration and RDP reconnaissance are quiet, less noticeable forms of reconnaissance behavior than port sweeps or port scans. As a result, attackers often feel they can use these tools with relatively low risk of detection.

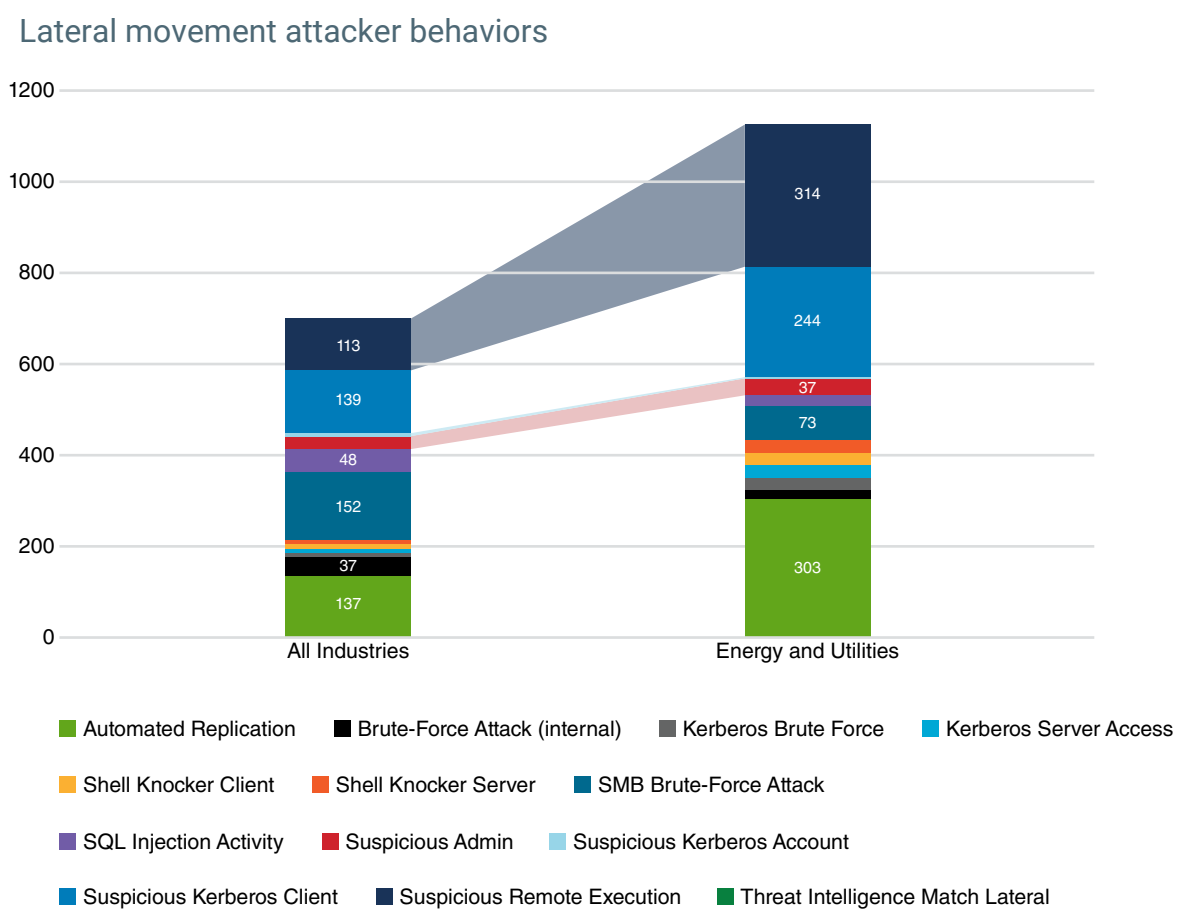


Figure 5: Lateral movement attacker behaviors in the energy and utilities industry per 10,000 host devices

Lateral movement inside a network exposes a larger attack surface to cybercriminals and substantially increases the risk of data acquisition and data exfiltration.

Unexplained and unusual patterns of use of host devices, domain controllers and services are involved in almost all major breaches. Attacks carried out by insiders will often exhibit unusual patterns of use as well.

The compromised host devices and services accessed provide perspective on the potential business impact. As reported by the TA18-074A alert issued by the DHS, the most common lateral movement behaviors inside energy and utilities companies were suspicious remote execution.

As shown in Figure 5, the Cognito platform detected 314 suspicious remote execution behaviors per 10,000 workloads and devices. The suspicious use of Kerberos accounts was detected two times per 10,000 host devices and workloads, while suspicious administrative activity was observed 37 times per 10,000 host devices and workloads.

Lateral movement via remote execution is a key element of many different attacks and the server message block (SMB) channel allows the copying of executables and executing them via remote procedure call (RPC). Systems that are authorized to perform remote execution should be monitored because they enable attackers to hide in plain sight.

A Kerberos account is suspicious when it is used differently than expected in one or more ways. This includes connecting to unusual domain controllers, using unusual host devices and accessing unusual services, or generating unusual volumes of Kerberos requests using normal domain controllers, usual host devices and usual services.

More importantly, administrative protocols are a favorite tool of attackers because they allow cybercriminals to move laterally inside networks where they have already established a durable foothold.

Because administrative connections are typically used in conjunction with administrative credentials, attackers often have unconstrained access to systems and data that are critical to energy and utilities organizations. Unexpected and unexplained administrative connections represent a huge potential risk in the lifecycle of a major breach.

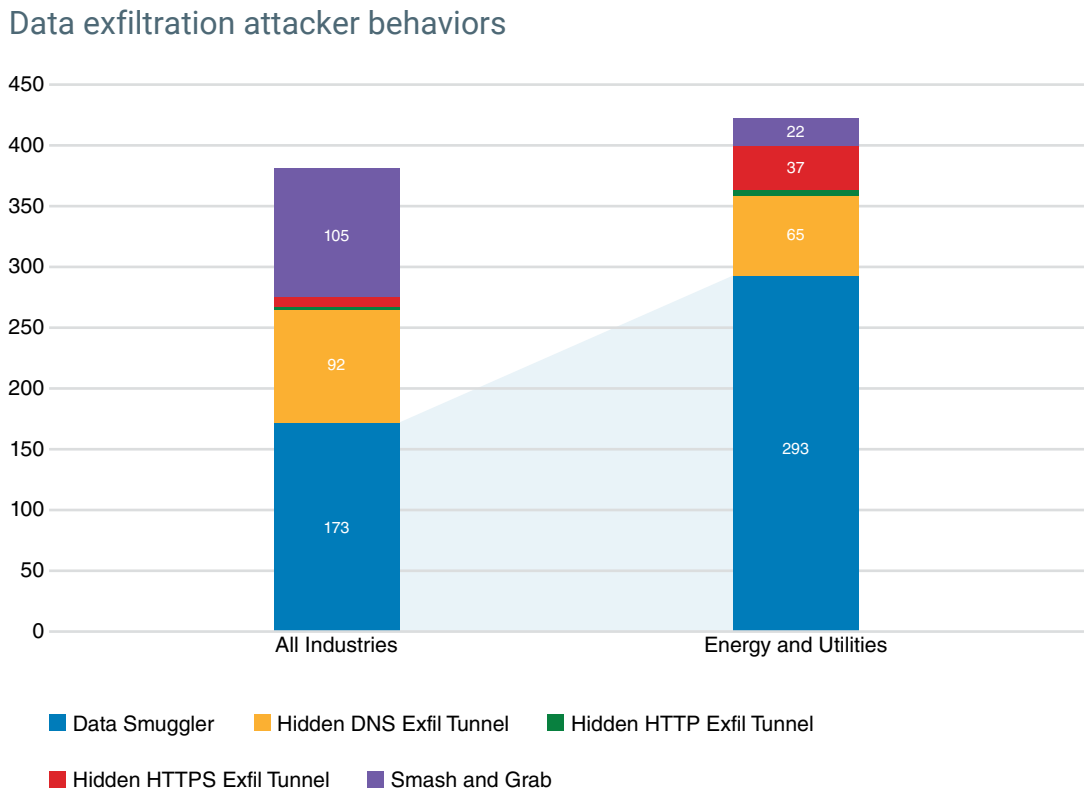


Figure 6: Exfiltration attacker behaviors in the energy and utilities industry per 10,000 host devices

Energy and utilities networks exhibit significant behaviors in which internal host devices acquire large amounts of data from one or more internal servers and send large amounts of data to an external system.

These behaviors alone do not necessarily indicate an attack. An attack is likely when exfiltration behaviors correlate with other attacker behaviors in different phases of the attack lifecycle, such as command and control, reconnaissance or lateral movement. It is also critical to ensure that systems communicate only to approved locations.

As shown in Figure 6, these exfiltration behaviors, described as data smuggler, were detected by the Cognito platform inside energy and utilities networks 293 times per 10,000 host devices and workloads.

To understand if these potential threat behaviors are of concern, the internal servers from which the data was retrieved can provide some indication of the type of data that was acquired. If those servers contain valuable information and the external service to which data was uploaded is not an IT-authorized service, the potential business risk is exceptionally high.

A chilling reminder to monitor the network for attacker behaviors

Monitoring the network for attacker behaviors may provide the only clues to tracking their steps since the attacker may have erased evidence on endpoints as well as logs.

Based on the TA18-074A alert released by the DHS about the Russian government attack campaign against energy and other critical infrastructure sectors, threat actors in multiple instances created new accounts on staging targets to perform cleanup operations.

The accounts were used to clear the following Windows event logs: System, security, terminal services, remote services, and audit. The threat actors also removed applications they installed while they were in the network along with any logs produced.

For example, the Fortinet client installed at one commercial facility was deleted along with the logs that were produced from its use. Finally, data generated by other accounts used on the accessed systems were deleted.

Threat actors cleaned up the target networks by deleting created screenshots and specific registry keys. Through forensic analysis, the DHS determined that threat actors deleted the registry key associated with a terminal server client that tracks connections made to remote systems. Threat actors also deleted all batch scripts, output text documents and tools they brought into the environment, such as *scr.exe*.

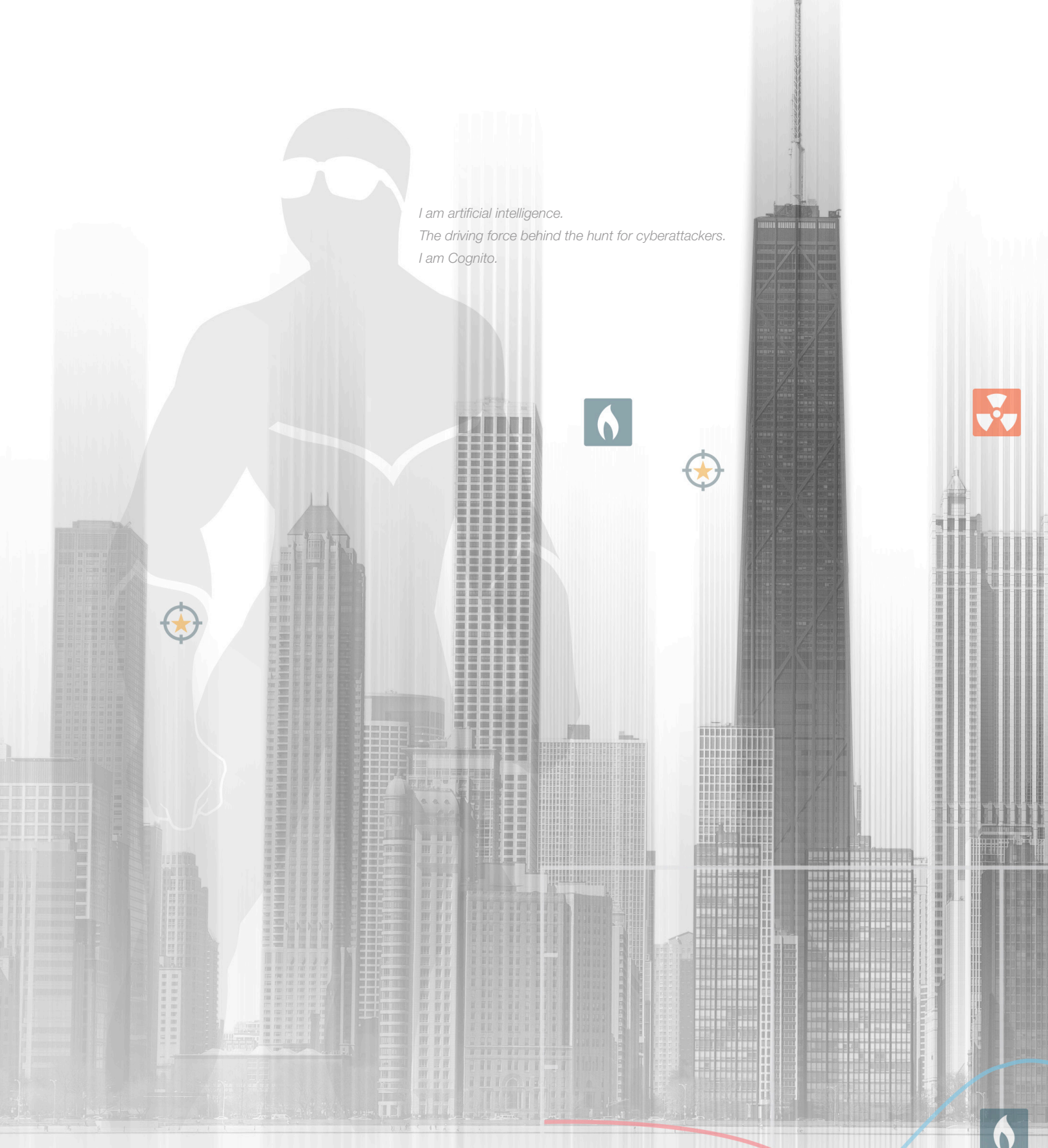
About the Cognito platform from Vectra

To combat attacks in the energy and utilities industry, the Cognito platform from Vectra inspects rich metadata from all network traffic to identify attacker behaviors in real time, even when cybercriminals try to cover their tracks.

The Cognito platform uses AI – including supervised and unsupervised machine learning techniques – to perform non-stop, automated threat detection. Always-learning behavioral models are driven by AI to quickly and efficiently find hidden and unknown attackers before they do damage. Cognito provides full visibility into attacker behaviors, from cloud and data center workloads to user and internet-of-things devices, leaving attackers with nowhere to hide.

Cognito Detect™ and its AI counterpart, Cognito Recall™, are the cornerstones of the Cognito platform. Cognito Detect automates the real-time detection of hidden attackers while giving Cognito Recall a logical starting point to perform AI-assisted threat hunting and conclusive incident investigations.

To learn more about other cyberattacker behaviors seen in real-world cloud, data center and enterprise environments, get the 2018 Black Hat Edition of the Attacker Behavior Industry Report from Vectra.



VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai