Overview

VECTRA®

The Cognito automated threat detection and response platform

HIGHLIGHTS

- Finds active cyberattackers inside cloud, data center and enterprise environments
- Automates security investigations with conclusive answers
- Persistently tracks threats across all phases of attack
- Monitors all traffic – internal and internet
- Analyzes logs from security systems, authentication systems and SaaS applications
- Covers all devices – any operating system, BYOD and IoT
- Secures all infrastructures – physical and virtual
- Integrates with leading SIEMs, firewalls, NAC, and endpoint solutions

Cognito™ from Vectra® is the fastest, most efficient way to find and stop cyberattackers in public clouds, private data centers and enterprise environments. It uses artificial intelligence to deliver real-time attack visibility and put attack details at your fingertips to empower immediate action.

By combining advanced machine learning techniques – including deep learning and neural networks – with always-learning behavioral models, Cognito quickly and efficiently finds hidden and unknown attackers before they do damage.

Cognito provides enterprise-wide visibility into hidden cyberattackers by analyzing all network traffic and logs from security systems, authentication systems and SaaS applications. This leaves attackers with nowhere to hide – from cloud and data center workloads to user and IoT devices.

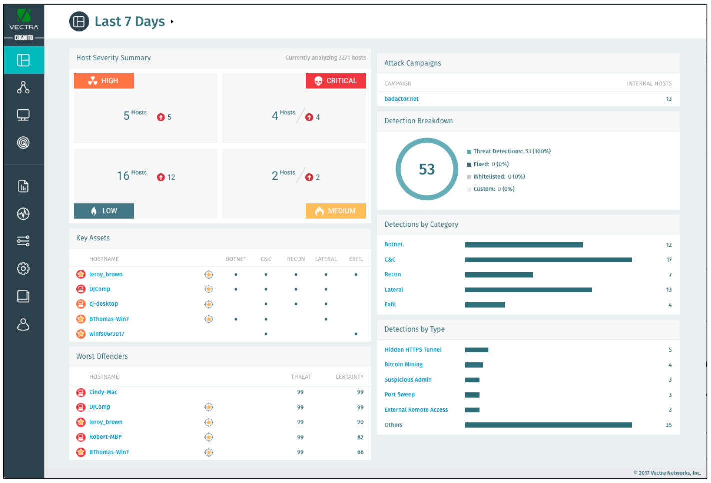
As part of the Cognito subscription, software updates with new threat detection algorithms are delivered to customers on a regular basis to ensure they are continuously protected from the latest advanced threats.

Security analyst in software

Cognito automates the hunt for cyberattackers, shows where they're hiding and tells you what they're doing. The highest-risk threats are instantly triaged, correlated to hosts and prioritized so security teams can respond faster to stop in-progress attacks and avert data loss.

By automating the manual, time-consuming analysis of security events, Cognito condenses weeks or months of work into minutes and reduces the security-analyst workload on threat investigations by 29x.

This enables security operations teams that are understaffed and under siege to stay ahead of cyberattackers and respond faster to hidden threats.



Host Severity Summary

Currently analyzing 3271 hosts

HIGH 5 Hosts ↑ 5	CRITICAL 4 Hosts / ↑ 4
16 Hosts ↑ 12 LOW	2 Hosts / ↑ 2 MEDIUM

Key Assets

HOSTNAME	BOTNET	C&C	RECON	LATERAL	EXFIL
leroy_brown	•	•	•	•	•
DJComp	•	•	•	•	
cj-desktop		•	•	•	
BThomas-Win7	•	•		•	
winfs06r3u17		•			•

Worst Offenders

HOSTNAME	THREAT	CERTAINTY
Cindy-Mac	99	99
DJComp	99	99
leroy_brown	99	90
Robert-MBP	99	82
BThomas-Win7	99	66

Attack Campaigns

CAMPAIGN	INTERNAL HOSTS
badactor.net	13

Detection Breakdown

53

- Threat Detections: 53 (100%)
- Fixed: 0 (0%)
- Whitelisted: 0 (0%)
- Custom: 0 (0%)

Detections by Category

Botnet	12
C&C	17
Recon	7
Lateral	13
Exfil	4

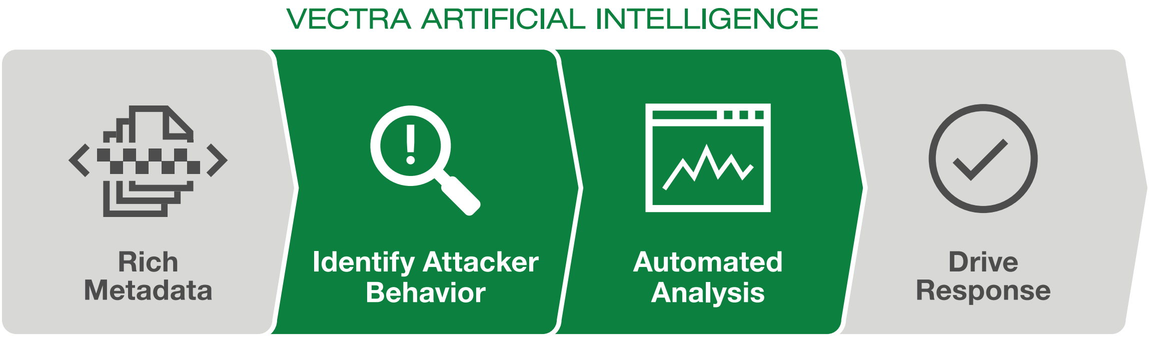
Detections by Type

Hidden HTTPS Tunnel	5
Bitcoin Mining	4
Suspicious Admin	3
Port Sweep	3
External Remote Access	3
Others	35

© 2017 Vectra Networks, Inc.

Attacker detections are instantly prioritized, scored and correlated to compromised host devices

How Cognito works



- Network traffic
- System, auth and SaaS logs
- IoCs (STIX)

- Machine learning
- Behavioral analytics
- Network effect

- Triage and correlate threats to hosts
- Prioritize hosts by risk
- Uncover attack campaigns

- Intuitive UI with rich context
- Enable automated response
- Firewall, endpoint, SIEM and NAC integration

Rich metadata

Cognito gives you real-time visibility into network traffic by extracting metadata from packets rather than performing deep packet inspection, enabling protection without prying.

Metadata analysis is applied to all internal (east-west) traffic, Internet-bound (north-south) traffic, virtual infrastructure, and cloud computing environment. Cognito identifies, tracks, and scores every IP-enabled device inside the network.

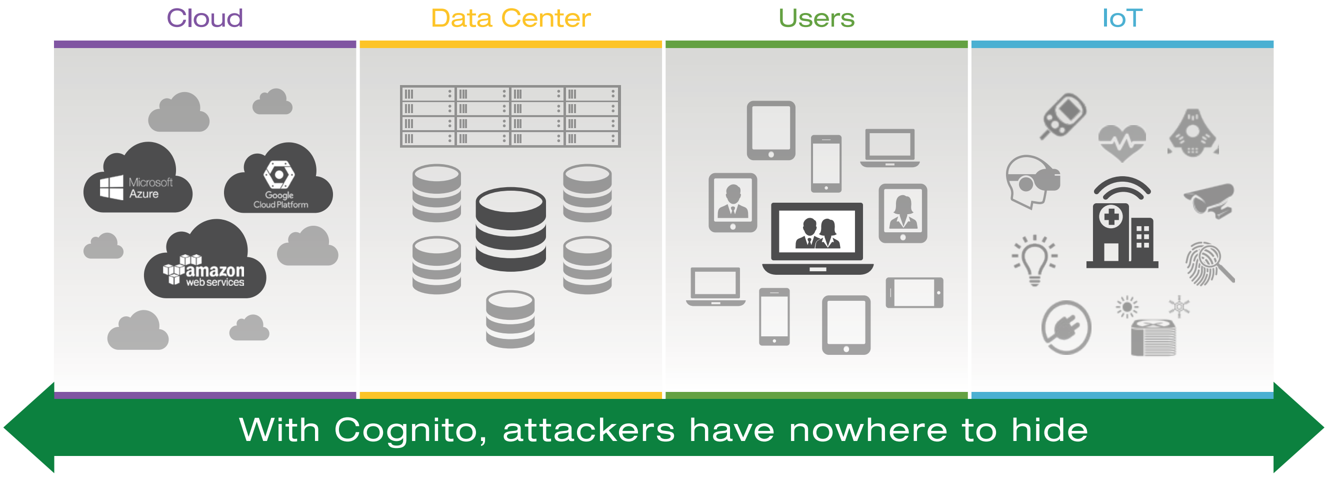
This visibility extends to laptops, servers, printers, BYOD and IoT devices as well as all operating systems and applications, including traffic between virtual workloads in data centers and the cloud, even SaaS applications.

System, authentication and SaaS logs provide context enrichment to network metadata analysis for accurate identification of systems and users.

Cognito uses STIX threat intelligence to detect threats based on known indicators of compromise derived from threat intelligence. These are correlated with other attacker behaviors to ensure pinpoint accuracy of host threat and certainty scores to prioritize risk.

Identify attacker behaviors

The collected metadata is analyzed with behavioral detection algorithms that spot hidden and unknown attackers. This exposes fundamental attacker behaviors in network traffic, such as remote access tools, hidden tunnels, backdoors, credential abuse, and internal reconnaissance and lateral movement.



Cognito provides threat detection coverage across the entire enterprise

Cognito continuously learns your local environment and tracks all physical and virtual hosts to reveal signs of compromised devices and insider threats. A wide range of cyberthreats are automatically detected in all phases of the attack kill-chain, including:

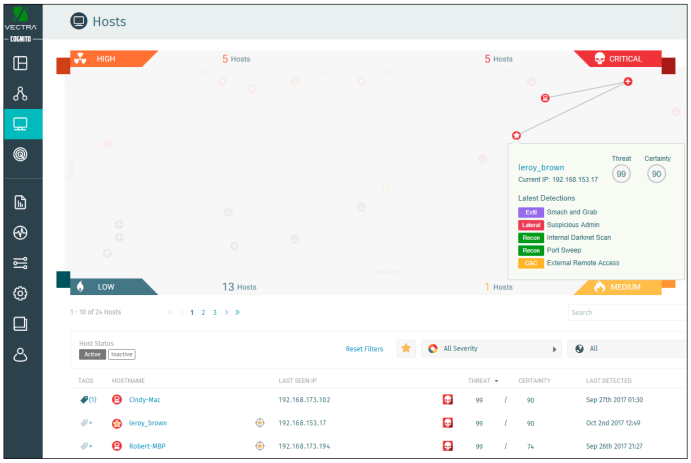
- Command-and-control and other hidden communications
- Internal reconnaissance
- Lateral movement
- Abuse of account credentials
- Data exfiltration
- Early indicators of ransomware activity
- Botnet monetization
- Attack campaigns, including the mapping of all hosts and their associated attack indicators

Cognito also monitors and detects suspicious access to critical assets by authorized employees, as well as policy violations related to the use of cloud storage, USB storage and other means of moving data out of the network.

Automated analysis

The Threat Certainty Index™ consolidates thousands of events and historical context to pinpoint hosts that pose the biggest threat.

Instead of generating more events to analyze, Cognito boils down mountains of data to show what matters most. Threat and certainty scores trigger notifications to your staff or a response from other enforcement points, SIEMs and forensic tools.



leroy_brown
Current IP: 192.168.153.17

Threat	Certainty
99	90

Latest Detections

Exfil	Smash and Grab
Lateral	Suspicious Admin
Recon	Internal Darknet Scan
Recon	Port Sweep
C&C	External Remote Access

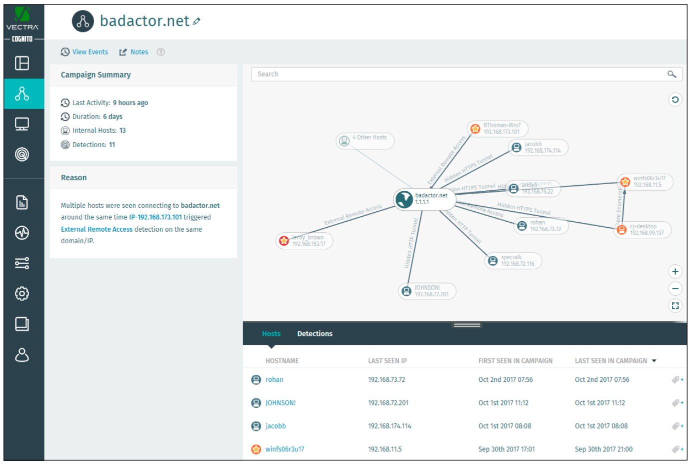
1 - 10 of 24 Hosts « ‹ 1 2 3 › »

TAGS	HOSTNAME	LAST SEEN IP	THREAT	CERTAINTY	LAST DETECTED
(1)	Cindy-Mac	192.168.173.102	99	90	Sep 27th 2017 01:30
+	leroy_brown	192.168.153.17	99	90	Oct 2nd 2017 12:49
+	Robert-MBP	192.168.173.194	99	74	Sep 26th 2017 21:27

The Vectra Threat Certainty Index

The Attack Campaigns feature further automates security detections by connecting the dots of related attacker behaviors and exposing the relationship between hosts across internal detections, external advanced command-and-control detections, and connectivity to common command-and-control infrastructures.

As attackers perform reconnaissance and move laterally from host to host in a network, Cognito correlates their behaviors across all involved hosts and detections and presents a synthesized view of the entire attack campaign.



Campaign Summary

Last Activity: 9 hours ago
Duration: 6 days
Internal Hosts: 13
Detections: 11

Reason

Multiple hosts were seen connecting to badactor.net around the same time IP-192.168.173.101 triggered External Remote Access detection on the same domain/IP.

HOSTNAME	LAST SEEN IP	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
rohan	192.168.73.72	Oct 2nd 2017 07:56	Oct 2nd 2017 07:56
JOHNSON!	192.168.72.201	Oct 1st 2017 11:12	Oct 1st 2017 11:12
jacobb	192.168.174.114	Oct 1st 2017 08:08	Oct 1st 2017 08:08
winfs06r3u17	192.168.11.5	Sep 30th 2017 17:01	Sep 30th 2017 21:00

Cognito presents a synthesized view of an entire attack campaign

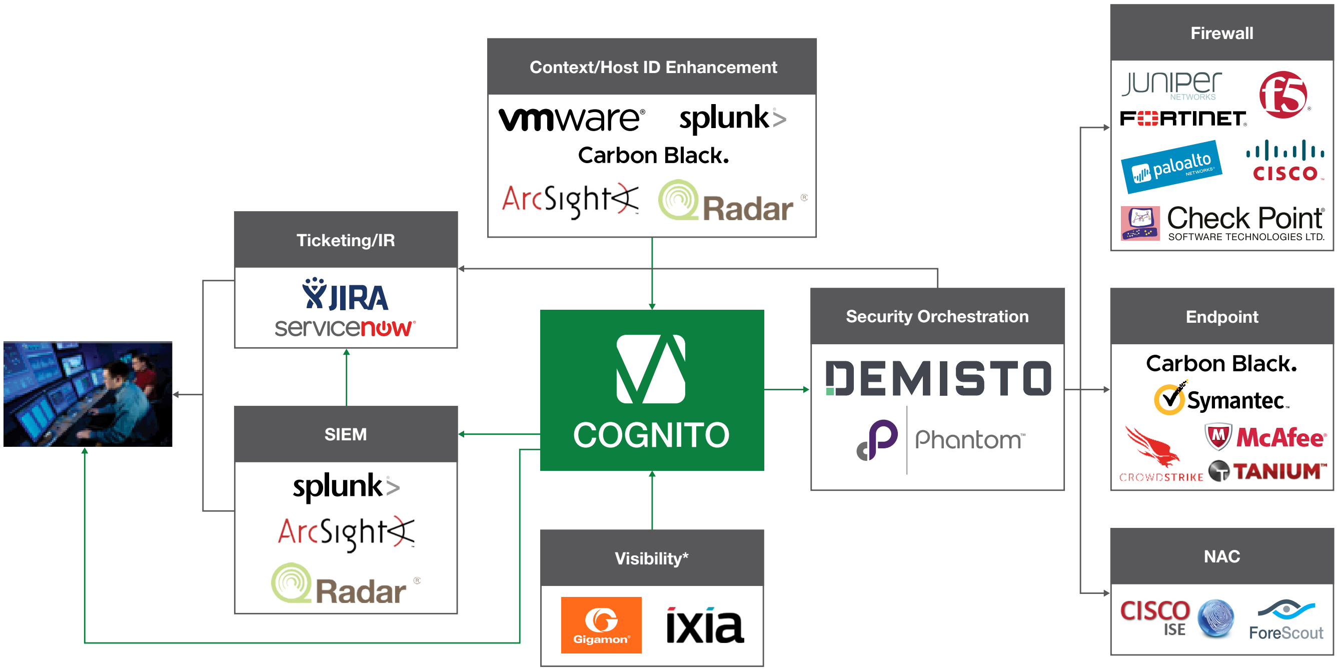
Cognito pivots to show views of hosts or related campaign detections, and analyzes event history spanning its entire lifetime to better understand the activity and full scope of attack.

Drive response

Respond quickly and decisively to threats by putting the most relevant information and context at your fingertips. Unlike security analytics products, Cognito eliminates manual investigations by automatically prioritizing and correlating threats with compromised hosts and key assets that are the target of an attack.

Cognito puts threat detection details – including host context, packet captures, and threat and certainty scores – within immediate reach.

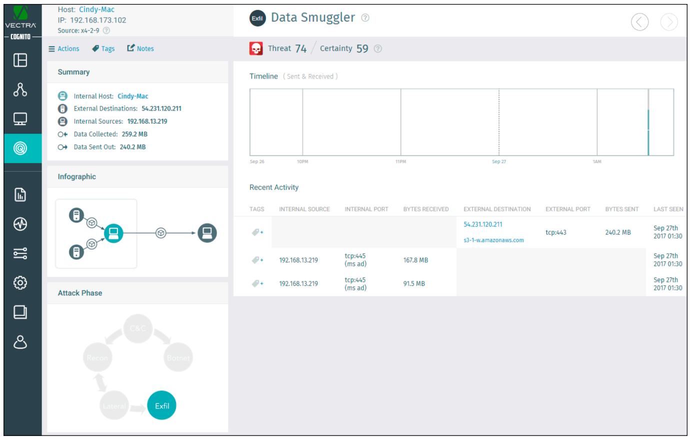
In addition, Cognito works with your next-generation firewalls, endpoint security, NAC, and other enforcement points to automatically block unknown and customized cyberattacks. Cognito also provides a clear starting point for threat investigations, which boosts the efficiency of SIEMs and forensic analysis tools.



*physical & cloud

Cognito works with widely used security enforcement points, SIEMs and forensic analysis tools

Security that thinks®



Host: Cindy-Mac
IP: 192.168.173.102
Source: x4-2-9

Data Smuggler

Threat 74 / Certainty 59

Summary

Internal Host: Cindy-Mac
External Destinations: 54.231.120.211
Internal Sources: 192.168.13.219
Data Collected: 259.2 MB
Data Sent Out: 240.2 MB

Infographic

Recent Activity

TAGS	INTERNAL SOURCE	INTERNAL PORT	BYTES RECEIVED	EXTERNAL DESTINATION	EXTERNAL PORT	BYTES SENT	LAST SEEN
+				54.231.120.211 s3-1-w.amazonaws.com	tcp:443	240.2 MB	Sep 27th 2017 01:30
+	192.168.13.219	tcp:445 (ms ad)	167.8 MB				Sep 27th 2017 01:30
+	192.168.13.219	tcp:445 (ms ad)	91.5 MB				Sep 27th 2017 01:30

Real-time detection of data exfiltration in progress

Security context that saves time

Cognito unburdens and empowers security operations teams that are understaffed. This is achieved by automating the time-consuming analysis of security events and eliminating the need to endlessly hunt for hidden threats.

Each detection is explained in detail, along with the underlying event and historical context that led to the detection. Security analysts can instantly view a connection map of any host to see other hosts the device is communicating with and how.

Cognito also provides on-demand access to metadata from captured packets for further forensic analysis. This gives security teams the proof and accuracy they need to take immediate, decisive action.

Strengthen your existing security infrastructure

Whether providing the intelligence to block a new class of threat with firewalls, endpoint security, NAC and other enforcement points, or providing a clear starting point for a more extensive search with SIEMs and forensic tools, Cognito gives you more value from existing security technologies.

Cognito integrates with leading endpoint security solutions to automatically add enriched context to investigations and enables security operations teams to isolate compromised host devices.

A robust API enables automated response and enforcement with virtually any security solution. Cognito also generates syslog messages and CEF logs for all detections as well as prioritized host scores. This makes Cognito much more than just another source of logs and provides an ideal trigger for investigations and workflows within your SIEM.

Full lifecycle detection of ransomware

Cognito detects ransomware campaigns against enterprises and other organizations across all phases of an attack. By monitoring all internal network traffic, Cognito identifies in seconds the fundamental behaviors of a ransomware attack as it attempts to take critical assets hostage.

In addition to detecting ransomware directly, Cognito detects ransomware precursors, including command-and-control traffic, network scans and spreading behavior that ransomware relies on to find and encrypt critical assets.

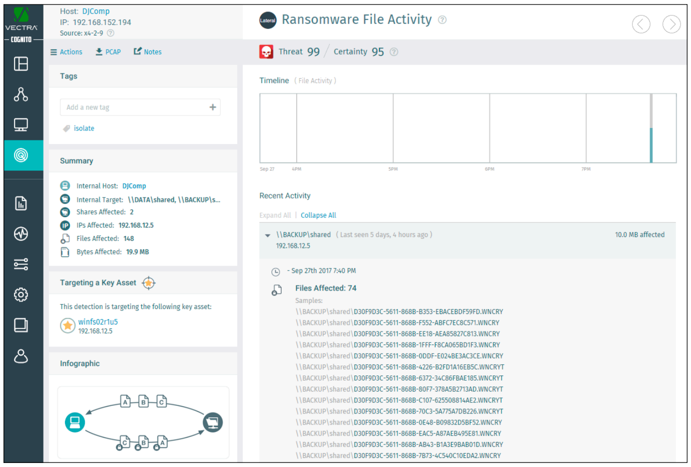
Watching the watchers

While attackers may initially compromise an end-user device, the real prize involves commandeering administrator or system credentials. Cognito goes beyond simple user-behavior monitoring to detect signs of compromised administrators.

Cognito tracks administrative protocols and learns the specific machines or jump systems that are used to manage specific hosts, servers and workloads. This vigilance quickly reveals when a cybercriminal attempts to use administrative credentials and protocols to escalate an attack on the network.

Native security for your private cloud

The private-cloud data center has become the heart and soul of many organizations, yet often remains a blind spot for security teams. Cognito persistently monitors critical data center applications, data, and infrastructure with the ability to detect even the most sophisticated attacks.



Host: DJComp
IP: 192.168.152.194
Source: x4-2-9

Ransomware File Activity

Threat 99 / Certainty 95

Tags

Add a new tag

isolate

Summary

Internal Host: DJComp
Internal Target: \\DATA\shared, \\BACKUP\s...
Shares Affected: 2
IPs Affected: 192.168.12.5
Files Affected: 148
Bytes Affected: 19.9 MB

Targeting a Key Asset

This detection is targeting the following key asset:
winfs02r1u5
192.168.12.5

Infographic

Timeline (File Activity)

Recent Activity

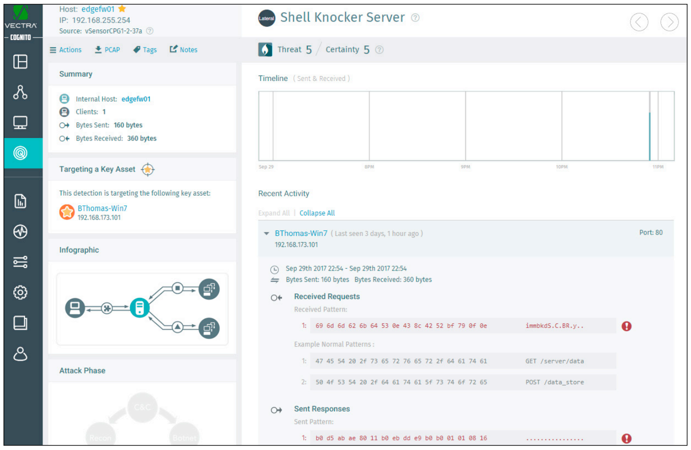
\\BACKUP\shared (Last seen 5 days, 4 hours ago) 10.0 MB affected
192.168.12.5

- Sep 27th 2017 7:40 PM

Files Affected: 74
Samples:

```
\\BACKUP\shared\D30F9D3C-5611-868B-B353-EBACEBDF59FD.WNCRY
\\BACKUP\shared\D30F9D3C-5611-868B-F552-ABFC7EC8C571.WNCRY
\\BACKUP\shared\D30F9D3C-5611-868B-EE18-AEA85827C813.WNCRY
\\BACKUP\shared\D30F9D3C-5611-868B-1FFF-F8CA065BD1F3.WNCRY
\\BACKUP\shared\D30F9D3C-5611-868B-0DDF-E024BE3AC3CE.WNCRY
\\BACKUP\shared\D30F9D3C-5611-868B-4226-B2FD1A16EB5C.WNCRYT
\\BACKUP\shared\D30F9D3C-5611-868B-6372-34C86FBAE185.WNCRYT
\\BACKUP\shared\D30F9D3C-5611-868B-80F7-378A5B2713AD.WNCRYT
\\BACKUP\shared\D30F9D3C-5611-868B-C107-625508814AE2.WNCRYT
\\BACKUP\shared\D30F9D3C-5611-868B-70C3-5A775A7DB226.WNCRYT
\\BACKUP\shared\D30F9D3C-5611-868B-0E48-B09832D5BF52.WNCRY
\\BACKUP\shared\D30F9D3C-5611-868B-EAC5-A87AEB495E81.WNCRY
\\BACKUP\shared\D30F9D3C-5611-868B-AB43-B1A3E9BAB01D.WNCRY
\\BACKUP\shared\D30F9D3C-5611-868B-7B73-4C540C10EDA2.WNCRY
```

The Cognito ransomware detection



Host: edgefw01
IP: 192.168.255.254
Source: vSensorCPG1-2-37a

Shell Knocker Server

Threat 5 / Certainty 5

Summary

Internal Host: edgefw01
Clients: 1
Bytes Sent: 160 bytes
Bytes Received: 360 bytes

Targeting a Key Asset

This detection is targeting the following key asset:
BThomas-Win7
192.168.173.101

Infographic

Attack Phase

Timeline (Sent & Received)

Recent Activity

BThomas-Win7 (Last seen 3 days, 1 hour ago) Port: 80
192.168.173.101

Sep 29th 2017 22:54 - Sep 29th 2017 22:54
Bytes Sent: 160 bytes Bytes Received: 360 bytes

Received Requests
Received Pattern:

```
1:  69 6d 6d 62 6b 64 53 0e 43 8c 42 52 bf 79 0f 0e    immbkdS.C.BR.y..
```

Example Normal Patterns :

```
1:  47 45 54 20 2f 73 65 72 76 65 72 2f 64 61 74 61    GET /server/data
2:  50 4f 53 54 20 2f 64 61 74 61 5f 73 74 6f 72 65    POST /data_store
```

Sent Responses
Sent Pattern:

```
1:  b0 d5 ab ae 80 11 b0 eb dd e9 b0 b0 01 01 08 16    ................
```

The Cognito Shell-Knocker detection

Some 80% of data center traffic never leaves the data center and is not monitored by traditional perimeter-based security. Cognito virtual sensors (vSensors) connect to any VMware vSwitch to ensure visibility into all traffic and detect threats passing between workloads in the virtual environment.

Cognito also integrates with VMware vCenter to provide an authoritative, always up-to-date view of your virtual environment. In fact, Cognito was first to bring together the required visibility, context and intelligence to find advanced attacks inside the data center.

Security from hardware to workload

Data center security goes beyond virtualization and includes the physical server hardware and low-level tools used to manage the data center. Cognito provides unprecedented threat detection that extends from the application layer down to the underlying hardware.

For example, the Cognito Port Knocking detection reveals servers that are compromised by a rootkit, which could reside below the physical operating system itself. In addition, Cognito monitors and detects the improper use of low-level management protocols such as IPMI and iDRAC.

Normally used by administrators for infrastructure-lights-out management of server hardware, these protocols are increasingly targeted by attackers because they give an always-on backdoor into the virtual environment yet are not logged and are rarely monitored by security.

Unifying data center operations

Modern data centers require constant coordination between networking, application development, virtualization teams, and of course, the security team. Cognito makes it easy for all groups to remain in sync and retain full visibility into the virtual environment, even when workloads are constantly on the move.

Cognito visually displays the connections between all workloads and the type of traffic flowing between them. With full VMware vCenter integration, Cognito provides an always up-to-date view of the environment and alerts about any assets that are not monitored for threats.

VECTRA®
Security that thinks.®

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