NETSCOUT Omnis IDS in Action Use Case – Exporting Events to Security Ecosystem to Troubleshoot Ursnif Malware

A new breed of cybersecurity threats has garnered extensive media coverage, with some industry reports citing a 900% increase in malware instances in calendar year 2020.

However, as described in this Use Case, a malware attack need not be part of this new breed of cybersecurity threats in order to impair business service performance. Lastly, we know that it's not if, but when the events happen, and whether organizations are truly prepared to address those events rapidly, succinctly, and with repeatable processes.

For the Security Operations (SecOps) team profiled in this Use Case, the NETSCOUT Omnis Intrusion Detection System (Omnis IDS) improved the efficiency of their malware identification and response processes. Omnis IDS also enabled SecOps analysts to use established workflows in their Splunk Enterprise security information event management (SIEM) remediation tool by enabling the universal forwarder to export events to Splunk for complete visibility and correlation with other security systems.

Issue

As part of their daily network monitoring activities, the company's SecOps team identified a potential security event, which prompted issuance of associated service ticket.

In response, a front-line Tier 1 Security Analyst used the NETSCOUT® Omnis™ IDS to conduct preliminary investigation into this event, recognizing that solution allows for effective and timely event response as incidents occur, which is critically important to SecOps teams everywhere.

Impact

Given the location of security event across data center operations and the user's information regarding the impact on host server performance, transaction delays associated with this issue could result in lost productivity or, in a worst-case scenario, service downtime.

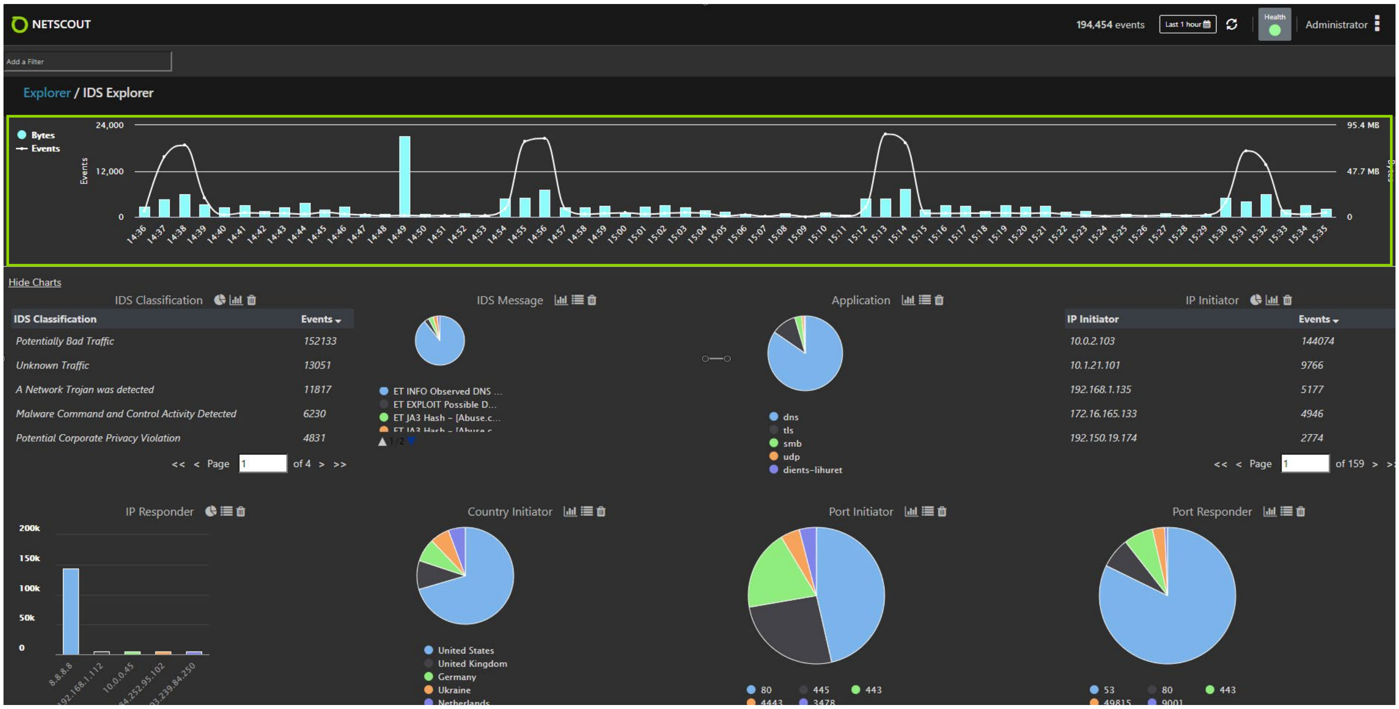
Troubleshooting

Accessing network events data aggregated by Omnis™ IDS Sensors deployed across the company's network, the Tier 1 Analyst commenced the investigation workflow by using the Omnis™ IDS Explorer Timeline, Filter and Search, and Total Events Counter features.

As part of this initial investigation, the Tier 1 Analyst contacted the internal user identified as potentially being impacted by this event. While this user reported issues with a host server running sluggishly (even confirming or affirming the host's IP address), the employee could not identify any recent actions or configuration changes that could be linked to potential root cause.

Even at this initial stage of the investigation workflow, using Omnis IDS, the Tier 1 Analyst could see there was a high number of events in the general report timeframe identified in the service ticket – nearly 200,000 of them, to be exact. As exhibited in Figure 2, however, a high volume of them were associated with two IP addresses, with Omnis IDS immediately easing the workflow for the Tier 1 analyst as a result.

Narrowing the IDS Explorer event timeline to correspond to the user-reported service issue enabled the Security Analyst to see relevant details associated with the host server IP address (10.1.21.101) initially shared by the user and recorded in the service ticket.



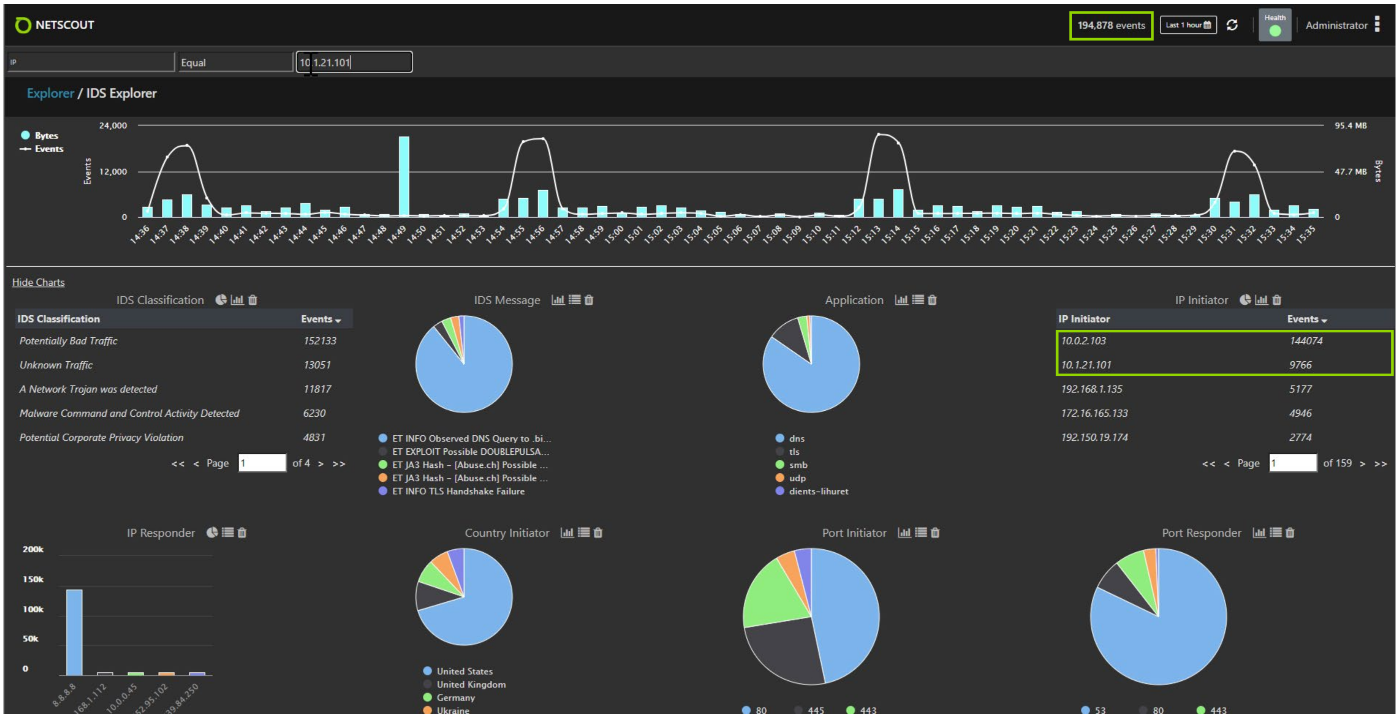
IDS Classification	Events
Potentially Bad Traffic	152133
Unknown Traffic	13051
A Network Trojan was detected	11817
Malware Command and Control Activity Detected	6230
Potential Corporate Privacy Violation	4831

<< < Page 1 of 4 > >>

IP Initiator	Events
10.0.2.103	144074
10.1.21.101	9766
192.168.1.135	5177
172.16.165.133	4946
192.150.19.174	2774

<< < Page 1 of 159 > >>

Figure 1: The front-line Tier 1 Analyst used Omnis IDS to commence the initial investigation workflow, with IDS Explorer providing a Timeline of Events and Bytes (upper panel), a Filter and Attribute window (for quick access to events and threats), and a Total Events Counter (for a given timeframe).



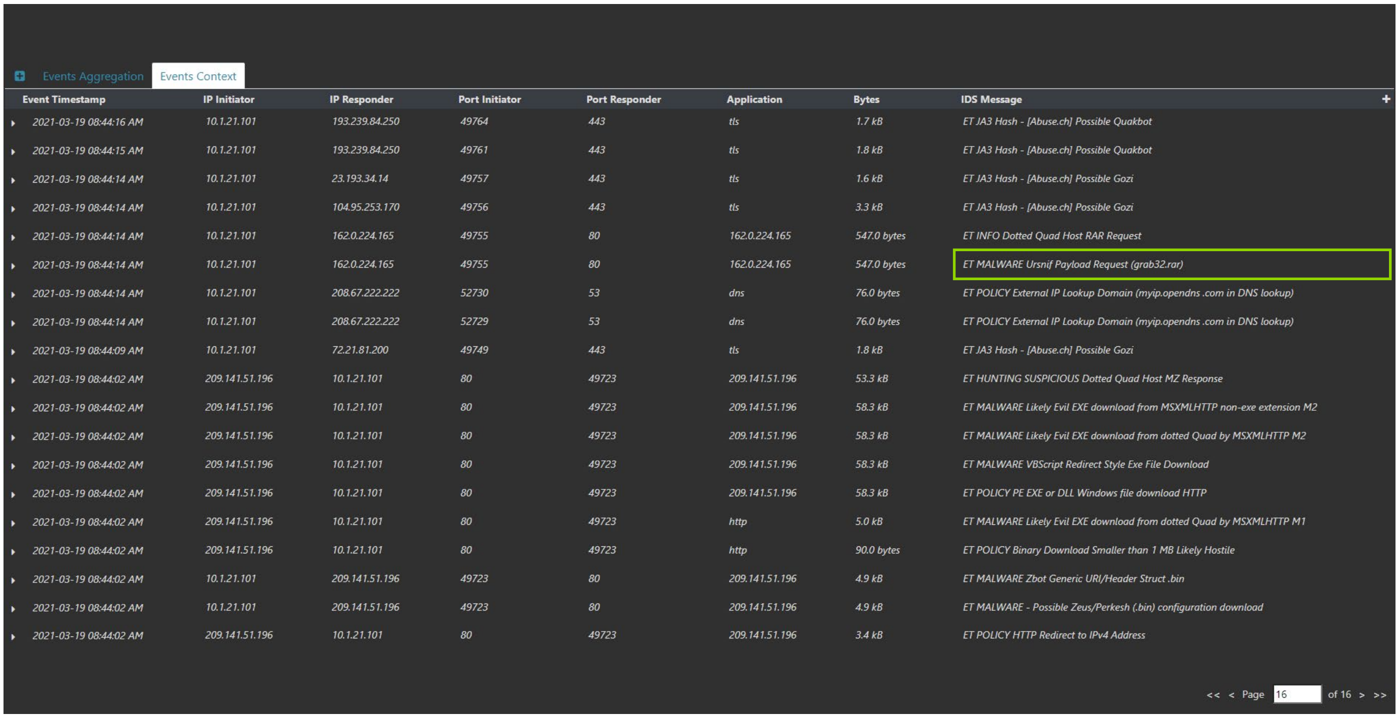
IDS Classification	Events
Potentially Bad Traffic	152133
Unknown Traffic	13051
A Network Trojan was detected	11817
Malware Command and Control Activity Detected	6230
Potential Corporate Privacy Violation	4831

<< < Page 1 of 4 > >>

IP Initiator	Events
10.0.2.103	144074
10.1.21.101	9766
192.168.1.135	5177
172.16.165.133	4946
192.150.19.174	2774

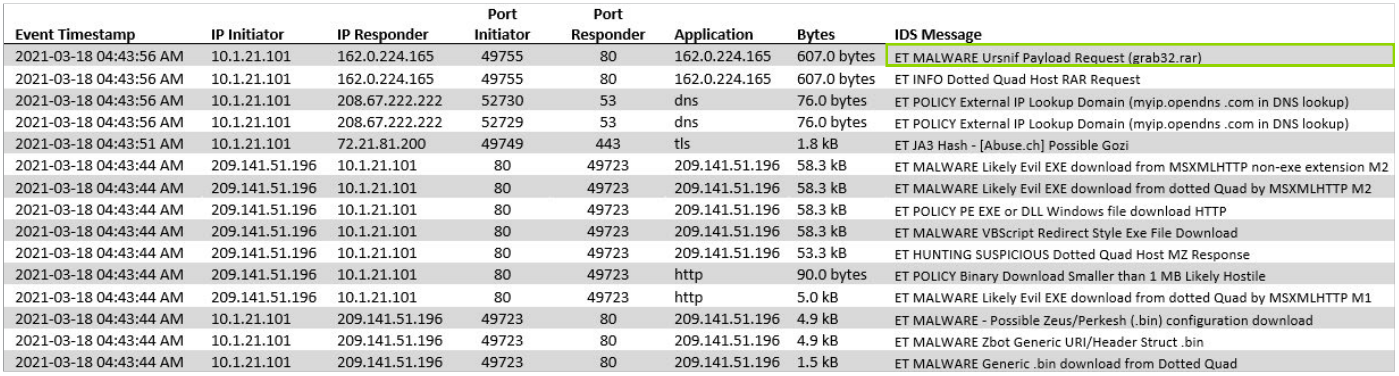
<< < Page 1 of 159 > >>

Figure 2: While the number of events displayed by the IDS Explorer's Event Counter was high, the IP Initiator widget on the lower right panel showed high volumes of them were associated with IP addresses 10.1.21.101 and 10.0.2.103.



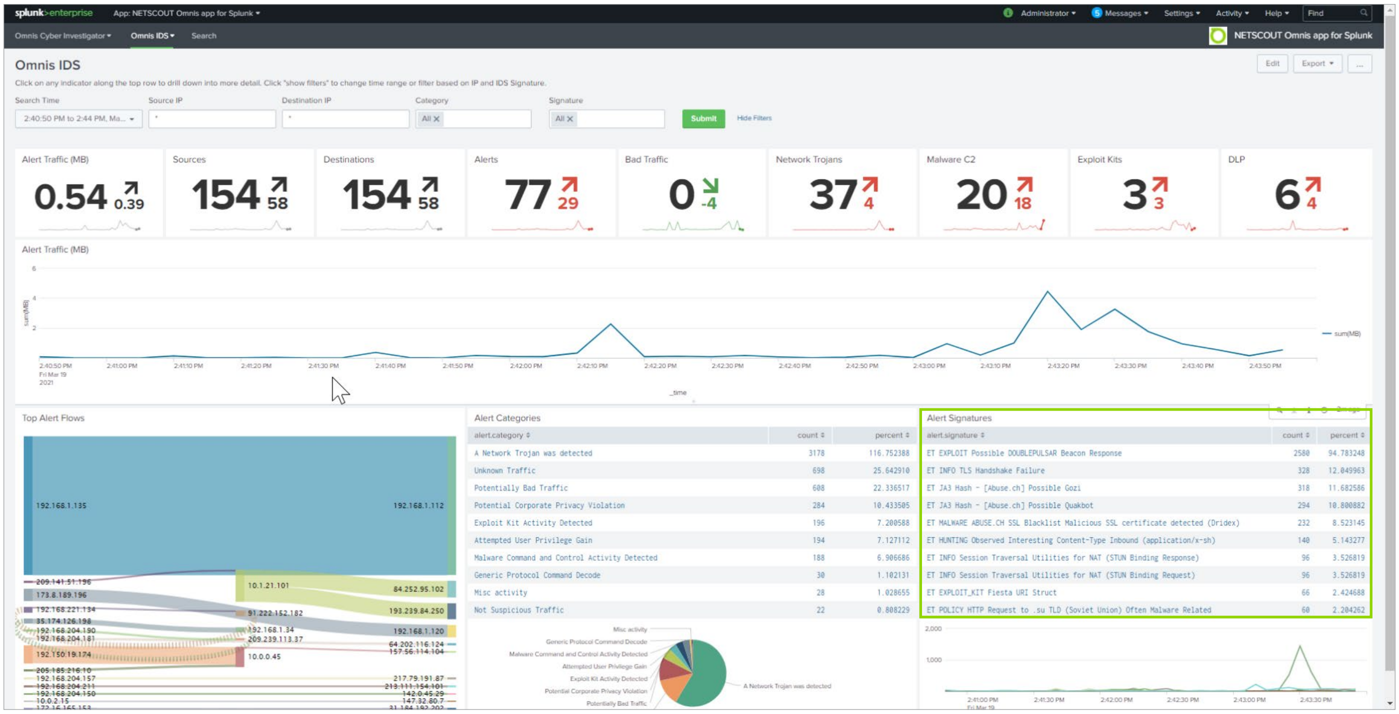
Event Timestamp	IP Initiator	IP Responder	Port Initiator	Port Responder	Application	Bytes	IDS Message
2021-03-19 08:44:16 AM	10.1.21.101	193.239.84.250	49764	443	tls	1.7 kB	ET JA3 Hash - [Abuse.ch] Possible Quakbot
2021-03-19 08:44:15 AM	10.1.21.101	193.239.84.250	49761	443	tls	1.8 kB	ET JA3 Hash - [Abuse.ch] Possible Quakbot
2021-03-19 08:44:14 AM	10.1.21.101	23.193.34.14	49757	443	tls	1.6 kB	ET JA3 Hash - [Abuse.ch] Possible Gozi
2021-03-19 08:44:14 AM	10.1.21.101	104.95.253.170	49756	443	tls	3.3 kB	ET JA3 Hash - [Abuse.ch] Possible Gozi
2021-03-19 08:44:14 AM	10.1.21.101	162.0.224.165	49755	80	162.0.224.165	547.0 bytes	ET INFO Dotted Quad Host RAR Request
2021-03-19 08:44:14 AM	10.1.21.101	162.0.224.165	49755	80	162.0.224.165	547.0 bytes	ET MALWARE Ursnif Payload Request (grab32.rar)
2021-03-19 08:44:14 AM	10.1.21.101	208.67.222.222	52730	53	dns	76.0 bytes	ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)
2021-03-19 08:44:14 AM	10.1.21.101	208.67.222.222	52729	53	dns	76.0 bytes	ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)
2021-03-19 08:44:09 AM	10.1.21.101	72.21.81.200	49749	443	tls	1.8 kB	ET JA3 Hash - [Abuse.ch] Possible Gozi
2021-03-19 08:44:02 AM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	53.3 kB	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response
2021-03-19 08:44:02 AM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	58.3 kB	ET MALWARE Likely Evil EXE download from MSXMLHTTP non-exe extension M2
2021-03-19 08:44:02 AM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	58.3 kB	ET MALWARE Likely Evil EXE download from dotted Quad by MSXMLHTTP M2
2021-03-19 08:44:02 AM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	58.3 kB	ET MALWARE VBScript Redirect Style Exe File Download
2021-03-19 08:44:02 AM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	58.3 kB	ET POLICY PE EXE or DLL Windows file download HTTP
2021-03-19 08:44:02 AM	209.141.51.196	10.1.21.101	80	49723	http	5.0 kB	ET MALWARE Likely Evil EXE download from dotted Quad by MSXMLHTTP M1
2021-03-19 08:44:02 AM	209.141.51.196	10.1.21.101	80	49723	http	90.0 bytes	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
2021-03-19 08:44:02 AM	10.1.21.101	209.141.51.196	49723	80	209.141.51.196	4.9 kB	ET MALWARE Zbot Generic URI/Header Struct .bin
2021-03-19 08:44:02 AM	10.1.21.101	209.141.51.196	49723	80	209.141.51.196	4.9 kB	ET MALWARE - Possible Zeus/Perkesh (.bin) configuration download
2021-03-19 08:44:02 AM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	3.4 kB	ET POLICY HTTP Redirect to IPv4 Address

Figure 3: The IDS Explorer Event List reflected the entire kill chain of techniques used to accomplish their tactic. This composite view of malicious traffic for techniques was presented in chronological order, including the Ursnif malware highlighted in the IDS Message panel on the right.



Event Timestamp	IP Initiator	IP Responder	Port Initiator	Port Responder	Application	Bytes	IDS Message
2021-03-18 04:43:56 AM	10.1.21.101	162.0.224.165	49755	80	162.0.224.165	607.0 bytes	ET MALWARE Ursnif Payload Request (grab32.rar)
2021-03-18 04:43:56 AM	10.1.21.101	162.0.224.165	49755	80	162.0.224.165	607.0 bytes	ET INFO Dotted Quad Host RAR Request
2021-03-18 04:43:56 AM	10.1.21.101	208.67.222.222	52730	53	dns	76.0 bytes	ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)
2021-03-18 04:43:56 AM	10.1.21.101	208.67.222.222	52729	53	dns	76.0 bytes	ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)
2021-03-18 04:43:51 AM	10.1.21.101	72.21.81.200	49749	443	tls	1.8 kB	ET JA3 Hash - [Abuse.ch] Possible Gozi
2021-03-18 04:43:44 AM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	58.3 kB	ET MALWARE Likely Evil EXE download from MSXMLHTTP non-exe extension M2
2021-03-18 04:43:44 AM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	58.3 kB	ET MALWARE Likely Evil EXE download from dotted Quad by MSXMLHTTP M2
2021-03-18 04:43:44 AM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	58.3 kB	ET POLICY PE EXE or DLL Windows file download HTTP
2021-03-18 04:43:44 AM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	58.3 kB	ET MALWARE VBScript Redirect Style Exe File Download
2021-03-18 04:43:44 AM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	53.3 kB	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response
2021-03-18 04:43:44 AM	209.141.51.196	10.1.21.101	80	49723	http	90.0 bytes	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
2021-03-18 04:43:44 AM	209.141.51.196	10.1.21.101	80	49723	http	5.0 kB	ET MALWARE Likely Evil EXE download from dotted Quad by MSXMLHTTP M1
2021-03-18 04:43:44 AM	10.1.21.101	209.141.51.196	49723	80	209.141.51.196	4.9 kB	ET MALWARE - Possible Zeus/Perkesh (.bin) configuration download
2021-03-18 04:43:44 AM	10.1.21.101	209.141.51.196	49723	80	209.141.51.196	4.9 kB	ET MALWARE Zbot Generic URI/Header Struct .bin
2021-03-18 04:43:44 AM	10.1.21.101	209.141.51.196	49723	80	209.141.51.196	1.5 kB	ET MALWARE Generic .bin download from Dotted Quad

Figure 4: The list exported list of events from IDS Explorer included highlighted IDS Message details on the Ursnif malware threat associated with the host server.



Omnis IDS

Click on any indicator along the top row to drill down into more detail. Click "show filters" to change time range or filter based on IP and IDS Signature.

Search Time	Source IP	Destination IP	Category	Signature
2:40:50 PM to 2:44 PM, Ma... ▾	*	*	All ✕	All ✕

Alert Traffic (MB)	Sources	Destinations	Alerts	Bad Traffic	Network Trojans	Malware C2	Exploit Kits	DLP
0.54 ↗ 0.39	154 ↗ 58	154 ↗ 58	77 ↗ 29	0 ↘ -4	37 ↗ 4	20 ↗ 18	3 ↗ 3	6 ↗ 4

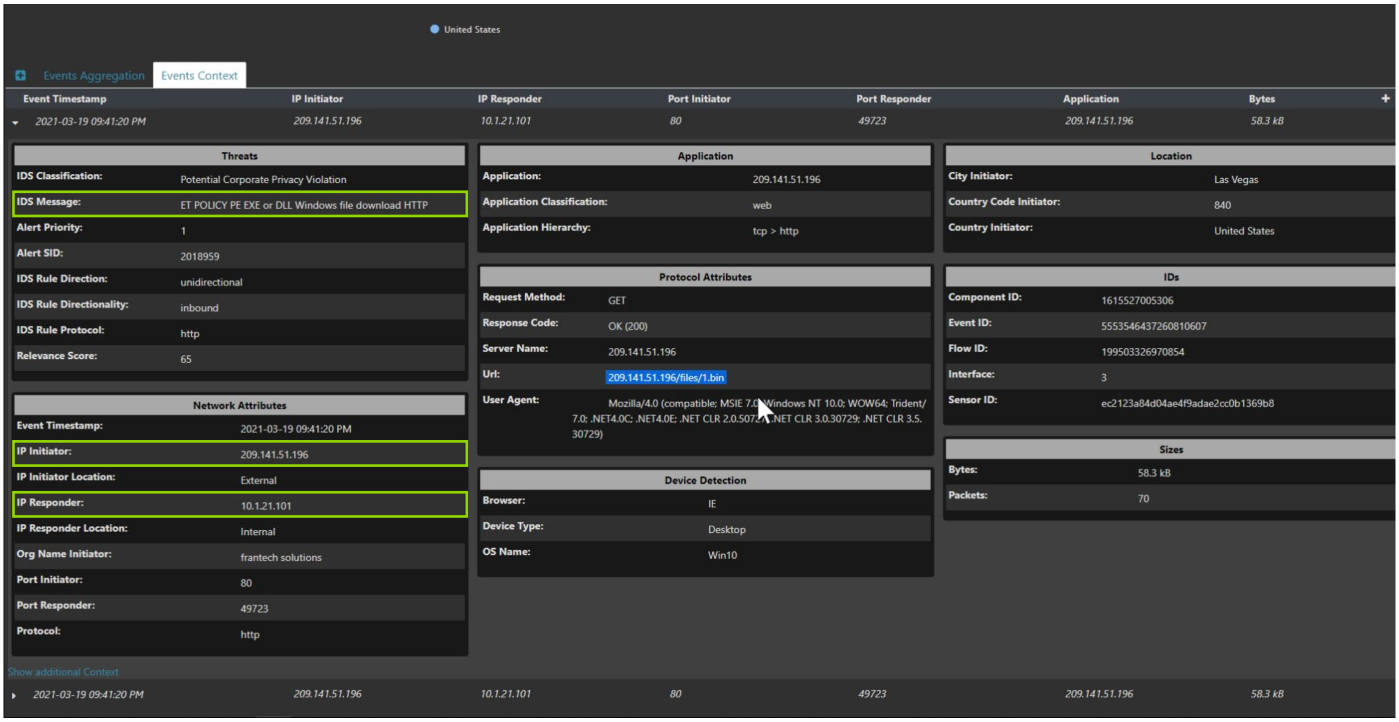
Alert Categories

alert.category	count	percent
A Network Trojan was detected	3178	116.752388
Unknown Traffic	698	25.642910
Potentially Bad Traffic	608	22.336517
Potential Corporate Privacy Violation	284	10.433505
Exploit Kit Activity Detected	196	7.200588
Attempted User Privilege Gain	194	7.127112
Malware Command and Control Activity Detected	188	6.906686
Generic Protocol Command Decode	30	1.102131
Misc activity	28	1.028655
Not Suspicious Traffic	22	0.808229

Alert Signatures

alert.signature	count	percent
ET EXPLOIT Possible DOUBLEPULSAR Beacon Response	2580	94.783248
ET INFO TLS Handshake Failure	328	12.049963
ET JA3 Hash - [Abuse.ch] Possible Gozi	318	11.682586
ET JA3 Hash - [Abuse.ch] Possible Quakbot	294	10.800882
ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	232	8.523145
ET HUNTING Observed Interesting Content-Type Inbound (application/x-sh)	140	5.143277
ET INFO Session Traversal Utilities for NAT (STUN Binding Response)	96	3.526819
ET INFO Session Traversal Utilities for NAT (STUN Binding Request)	96	3.526819
ET EXPLOIT_KIT Fiesta URI Struct	66	2.424688
ET POLICY HTTP Request to .su TLD (Soviet Union) Often Malware Related	60	2.204262

Figure 5: The Splunk SIEM interface includes integrated Omnis IDS event details in the lower right panel of this example screen.



Event Timestamp	IP Initiator	IP Responder	Port Initiator	Port Responder	Application	Bytes
▾ 2021-03-19 09:41:20 PM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	58.3 kB

Threats

IDS Classification:	Potential Corporate Privacy Violation
IDS Message:	ET POLICY PE EXE or DLL Windows file download HTTP
Alert Priority:	1
Alert SID:	2018959
IDS Rule Direction:	unidirectional
IDS Rule Directionality:	inbound
IDS Rule Protocol:	http
Relevance Score:	65

Network Attributes

Event Timestamp:	2021-03-19 09:41:20 PM
IP Initiator:	209.141.51.196
IP Initiator Location:	External
IP Responder:	10.1.21.101
IP Responder Location:	Internal
Org Name Initiator:	frantech solutions
Port Initiator:	80
Port Responder:	49723
Protocol:	http

Application

Application:	209.141.51.196
Application Classification:	web
Application Hierarchy:	tcp > http

Protocol Attributes

Request Method:	GET
Response Code:	OK (200)
Server Name:	209.141.51.196
Url:	209.141.51.196/files/1.bin
User Agent:	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)

Device Detection

Browser:	IE
Device Type:	Desktop
OS Name:	Win10

Location

City Initiator:	Las Vegas
Country Code Initiator:	840
Country Initiator:	United States

IDs

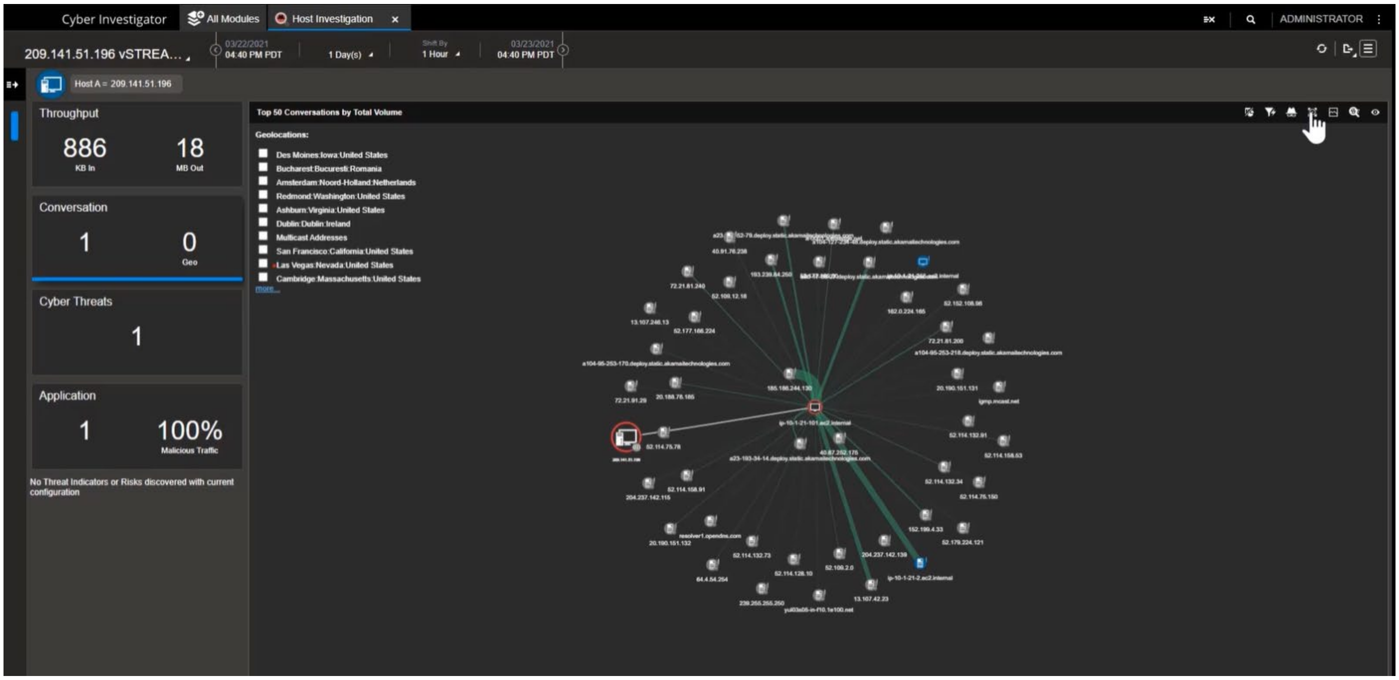
Component ID:	1615527005306
Event ID:	5553546437260810607
Flow ID:	199503326970854
Interface:	3
Sensor ID:	ec2123a84d04ae4f9adae2cc0b1369b8

Sizes

Bytes:	58.3 kB
Packets:	70

Event Timestamp	IP Initiator	IP Responder	Port Initiator	Port Responder	Application	Bytes
▸ 2021-03-19 09:41:20 PM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	58.3 kB

Figure 6: The IDS Explorer provided event context to the Tier 2 Analyst to confirm a malicious binary download had occurred, including the highlighted details regarding emerging threats signature (upper left panel), source and destination IP (lower left panel), and conclusive event evidence (center panel).



Throughput

886 KB In | 18 MB Out

Conversation

1 | 0 Geo

Cyber Threats

1

Application

1 | 100% Malicious Traffic

No Threat Indicators or Risks discovered with current configuration

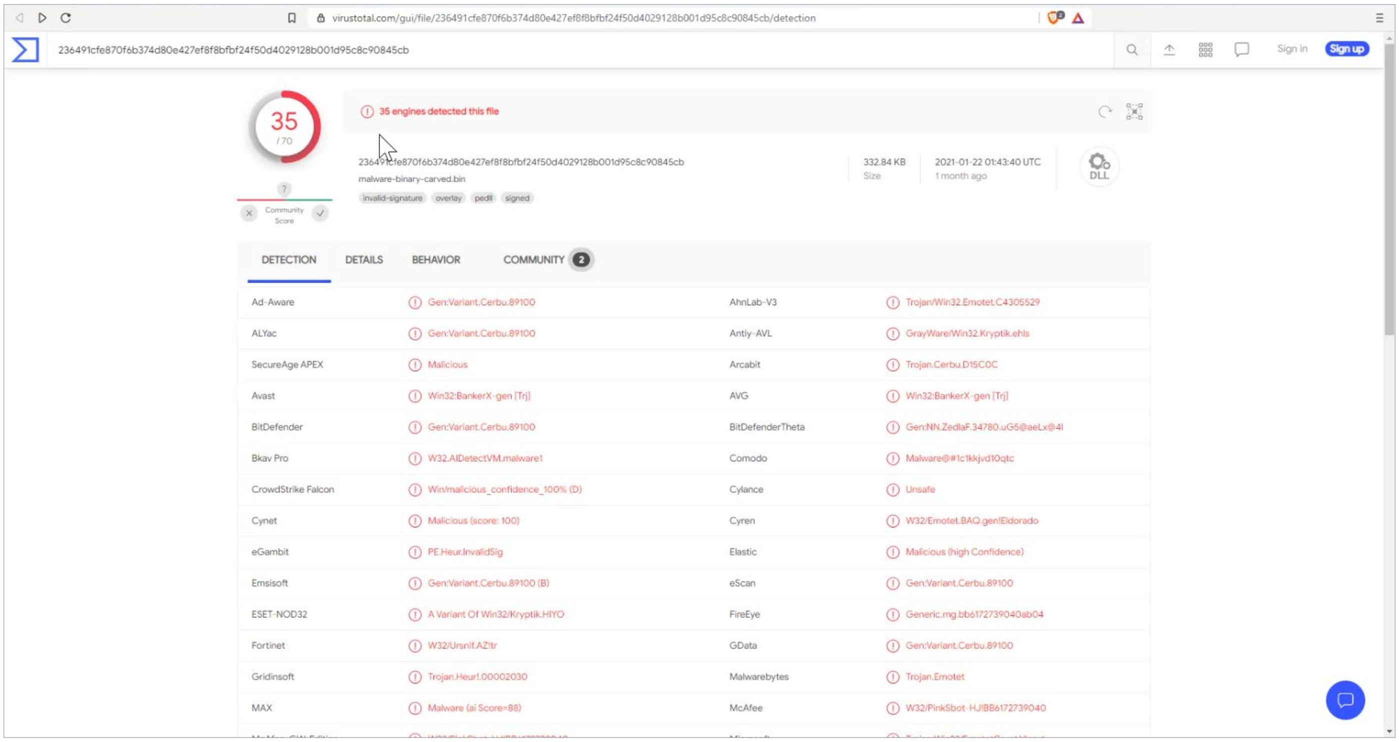
Top 50 Conversations by Total Volume

Geolocations:

- □ Des Moines:Iowa:United States
- □ Bucharest:Bucuresti:Romania
- □ Amsterdam:Noord-Holland:Netherlands
- □ Redmond:Washington:United States
- □ Ashburn:Virginia:United States
- □ Dublin:Dublin:Ireland
- □ Multicast Addresses
- □ San Francisco:California:United States
- □ Las Vegas:Nevada:United States
- □ Cambridge:Massachusetts:United States

more...

Figure 7: Omnis Cyber Intelligence provided the Tier 3 Analyst with an expanded view of all hosts, including listing the containment field, good vs. threat traffic, and a GeoIP list of Top 10.



virustotal.com/gui/file/236491cfe870f6b374d80e427ef8f8bfbf24f50d4029128b001d95c8c90845cb/detection

236491cfe870f6b374d80e427ef8f8bfbf24f50d4029128b001d95c8c90845cb

35 / 70

35 engines detected this file

236491cfe870f6b374d80e427ef8f8bfbf24f50d4029128b001d95c8c90845cb
malware-binary-carved.bin
invalid-signature overlay pedll signed

332.84 KB Size

2021-01-22 01:43:40 UTC 1 month ago

Ad-Aware	Gen:Variant.Cerbu.89100	AhnLab-V3	Trojan/Win32.Emotet.C4305529
ALYac	Gen:Variant.Cerbu.89100	Antiy-AVL	GrayWare/Win32.Kryptik.ehls
SecureAge APEX	Malicious	Arcabit	Trojan.Cerbu.D15C0C
Avast	Win32:BankerX-gen [Trj]	AVG	Win32:BankerX-gen [Trj]
BitDefender	Gen:Variant.Cerbu.89100	BitDefenderTheta	Gen:NN.ZedlaF.34780.uG5@aeLx@4l
Bkav Pro	W32.AIDetectVM.malware1	Comodo	Malware@#1c1kkjvd10qtc
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Emotet.BAQ.gen!Eldorado
eGambit	PE.Heur.InvalidSig	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Cerbu.89100 (B)	eScan	Gen:Variant.Cerbu.89100
ESET-NOD32	A Variant Of Win32/Kryptik.HIYO	FireEye	Generic.mg.bb6172739040ab04
Fortinet	W32/Ursnif.AZ!tr	GData	Gen:Variant.Cerbu.89100
Gridinsoft	Trojan.Heur!.00002030	Malwarebytes	Trojan.Emotet
MAX	Malware (ai Score=88)	McAfee	W32/PinkSbot-HJ!BB6172739040

Figure 8: Omnis Cyber Intelligence confirmed presence of the Ursnif malware and evidence that many of the security ecosystem's cybersecurity tools had not detected it.

By entering an IDS Filter attribute using that IP address, the Tier 1 Analyst updated all the displayed events down to those only related to that specific IP address, with the workflow then involving reducing the time period to minutes to generate a smaller data set with which to work. As exhibited in Figure 3, the end result of this workflow involved IDS Explorer sequentially listing various events for the IP address, including details on threats and exploits.

Using Omnis IDS in this manner, the Tier 1 Analyst was able to access IDS classifications related to malicious traffic and quickly visualized in the IDS Message Details that this was an Ursnif malware instance associated with the host server.

Ursnif is a network trojan that exploits users' systems as part of re-purposed malware. Ursnif is of relevance to any SecOps team, with this malware surfacing in numerous attacks on Japanese banking institutions in 2018, as reported by the NETSCOUT® ATLAS® Security Engineering and Response Team (ASERT). At this stage of the investigation workflow, the Tier 1 Analyst provided an Omnis IDS Threat Summary for handoff to the Tier 2 Analyst managing incident response. As part of that Threat Summary, the Tier 1 Analyst forwarded list of events surrounding that threat (as exhibited in Figure 4).

At this point, the Tier 2 Security Analyst used the NETSCOUT Omnis Application for Splunk to leverage the company's long-established SecOps workflows for event aggregation, analysis, and reporting in their Splunk Enterprise SIEM solution. With this application, the Tier 2 Security Analyst could access all exported Omnis IDS event data in Splunk. With the export of Omnis IDS event data into the Security Operations ecosystem, the Tier 2 Analyst used existing user interface workflows, as well as trends and timelines, with the ability to pivot to the Omnis IDS solution. Of particular relevance, the Tier 2 Analyst had access to integrated Omnis IDS event details, including alert signatures (as exhibited in Figure 5.)

The Tier 2 Analyst then used Splunk to validate that the event details provided by Omnis IDS corresponded to related events within Splunk (including use of the same destination IP and Source IP), with the workflow subsequently transitioning from Splunk to Omnis IDS.

At this point, the Tier 2 Analyst used IDS Explorer to access the event details and validated that the internal host had in fact downloaded the malware (as exhibited in Figure 6).

Remediation

At this point in the workflow, the service ticketed was transitioned to a Tier 3 Security Analyst to commence remediation activities. Event details were forwarded to the company's NETSCOUT Omnis™ Cyber Intelligence solution, an enterprise-wide network threat and risk investigation platform, which enabled the Tier 3 Analyst to examine the Ursnif malware instance in the context of the company's cybersecurity policies and take necessary actions for containment and prevention of future occurrences.

The Tier 3 Analyst used the Omnis Cyber Intelligence host investigation interface to identify the cyberthreat, confirm a threat on the external host, and identify a compromised internal host. By contextually drilling down from the internal host icon displayed on the Omnis Cyber Intelligence interface, the Tier 3 Analyst expands the view to all hosts communicating with the internal host. This remediation workflow process enabled the Tier 3 Analyst to determine that the possible containment field needed to be expanded to factor collateral hosts.

In providing additional verification to the Tier 3 Analyst, the workflow then transitioned to include the Omnis Cyber Intelligence packet decode functionality, which confirmed the Ursnif-related file had been downloaded by the internal host. Using Omnis Cyber Intelligence, the Tier 3 Analyst forwarded a corresponding packet capture export to the Forensic Security team. In integrating across this additional layer of the security ecosystem, SecOps not only had executive-level visual confirmation of a current and active Ursnif malware, but evidence that only half of the company's cybersecurity solutions had detected that threat.

In this instance, SecOps revised the company's perimeter security policy, including updating their NETSCOUT Omnis AED threat detection and DDoS mitigation solution configured at the perimeter edge with a threat filter to mitigate all subsequent traffic and mitigation policy.

Additionally, SecOps was presented with the option to configure their Omnis Cyber Intelligence solution to use a block command to enable a "blocking host" change.

With these adjustments, the SecOps team had secured the company's perimeter policy to protect organizational resources.

Summary

In this case, the SecOps team was able to take advantage of Omnis IDS functionality and forward rich event data to Splunk, which enabled use of monitors, workflows, and dashboards familiar to them, while also helping to expedite the evaluation. In taking advantage of the company's investment in NETSCOUT's Omnis Cyber Intelligence and Omnis AED solutions, SecOps made necessary adjustments to organizational security policies to negate the impact of this malware threat and protect the company from future occurrences.

In this manner, Omnis IDS enabled the SecOps team to remediate this malware instance before it could possibly have resulted in taking business services offline.

NETSCOUT.

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us