Gigamon®

Gigamon ThreatINSIGHT

NETWORK SECURITY POSTURE REPORT

NORTHSHORE SCHOOL DISTRICT

June 15, 2020

Contents

Executive Summary

Gigamon ThreatINSIGHT network sensors collected network traffic between Sep 18, 2019 and Oct 17, 2019. Gigamon used the collected metadata to identify metrics and potential security risks that are present in the environment. The Network Security Posture findings are organized by the directionality of the relevant traffic (inbound, outbound, and internal traffic) and are assigned one of the following risk scores:

- **HIGH**: The observed activity indicates an ongoing security issue or significantly decreases the security posture of the organization's environment.
- **MODERATE**: The observed activity could lead to future security issues.
- **LOW**: The observed activity may not pose an immediate risk but does not follow best practices.

Inbound Traffic	Outbound Traffic		Internal Traffic
SSH Connections: 3 Host(s)	SSH Connections: 23 Host(s)	IRC Traffic: 1 Host(s)	EOL Windows: 117 Host(s)
RDP Connections: 1 Host(s)	Large Data Transfers: 75 Host(s)	3rd-Party Remote Access: 11 Host(s)	Deprecated SSL: 38 Host(s)
Open Ports: 14 Port(s)	Direct HTTP: 1,000+ Host(s)	Direct DNS: 1,000+ Host(s)	Outdated Browsers: 1,000+ Host(s)
Connection Rejections 100+ Port(s)	Direct SMTP: 314 Host(s)	External DNS Servers: 100+ Host(s)	Outdated Java: 34 Host(s)
	3rd-Party Data Storage: 124 Host(s)		

Network Security Posture Findings

Inbound Traffic

SSH Connections from External Hosts [HIGH]

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network and was designed as a replacement for Telnet. SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login and remote command execution, however other network services can be secured with SSH. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2[1].

Exposing the SSH service on a host to the Internet leaves the host vulnerable to brute-force attacks that could result in unauthorized remote access to the system. Such hosts should be reviewed to ensure they are securely configured.

Observed Activity

ThreatINSIGHT observed 3 internal host(s) with inbound SSH connections. The top ten internal hosts by number of connections are shown below. The top three external organizations for both successful and unsuccessful connections, and a summary of the results for each organization, are shown for each host. The results of the connection attempts are summarized in the Results column by showing the first letter of each result observed (Successful or Unsuccessful).

Target Host	Source Organizations	Results	Connections
[redacted]	TierPoint, LLC (US) CenturyLink Communications, LLC (US) Comcast Cable Communications, LLC (US) Midcontinent Communications (US) Charter Communications Inc (US)	U	611 211 29 5 2
[redacted]	University of Washington (US)	S	4
[redacted]	University of Washington (US)	S	4

Table 1: Top 10 Hosts with successful inbound SSH connections by number of Connections

Example IQL Query

```
ssh:src.internal = false AND ssh:dst.internal = true and auth_success = true GROUP BY dst.ip LIMIT 1000, src.asn.asn_org LIMIT 3
```

Recommended Remediation

Review inbound SSH connections for suspicious activity or traffic that does not match approved business activities, such as hosts with only Unsuccessful connections. Each external organization with successful connections should have a well-documented business justification. Review each host to ensure all software is up-to-date and that secure configurations are in place. If remote logins via username and password are enabled,

[1] "SSH - Wikipedia." https://en.wikipedia.org/wiki/Secure_Shell. Accessed 15 May 2018.

ensure strong passwords are in place or consider disabling user account logins in favor of using public-private key pairs to login to the host.

RDP Connections from External Hosts [HIGH]

Remote Desktop Protocol[2] (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to remotely connect to another host. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

This finding is focused on RDP servers that are exposed to the Internet. This is generally an undesired configuration, as it can expose sensitive information and increases the attack surface of an organization. Internet-facing services are also subject to regular brute-force attempts by scanners and compromised devices.

Observed Activity

ThreatINSIGHT observed 1 host(s) with inbound RDP connections from external hosts. The top ten internal hosts by number of connections are shown below. The top three external organizations, as well as a summary of the results and the top three user accounts used, are shown for each host.

The Results column summarizes the results of the attempted connections to each host. A single connection attempt can have one of three result values:

- Successful — encryption was not used, allowing for confirmation of success
- Encrypted — encryption was used, preventing confirmation of success or failure
- Unsuccessful — the connection failed with either an error or a failed authentication

The results of the connection attempts from one external organization to one internal asset are summarized in the Results column by showing the first letter of each category observed. For example, an 'S' indicates at least one Successful result was observed.

Target Host	Source Organizations	Results	Users	Connections
[redacted]	Excalibur Technology Corporation (US)	E	hello	3,591
	vanoppen.biz LLC (US)		hello	1,561
	Psychz Networks (US)		hello	1,535

Table 2: Top 10 Hosts with successful inbound RDP connections by number of Connections

Example Query

```
rdp:src.internal = false AND rdp:dst.internal = true GROUP BY dst.ip LIMIT 1000, src.asn.asn_org LIMIT 3
```

Recommended Remediation

Review inbound RDP connections for suspicious activity or traffic that does not match approved business activities, such as hosts with only Unsuccessful connections. Enforce encryption on hosts with Successful (unencrypted) connections. Finally, utilize a VPN to provide access to the network and block all inbound RDP connections with a firewall rule.

[2] "Remote Desktop Protocol - Wikipedia." https://en.wikipedia.org/wiki/Remote_Desktop_Protocol. 15 May 2018.

Uncommon Open Ports [MODERATE]

An open port is a port that the perimeter firewall allows communications to flow through from external hosts to internal hosts. A small set of ports are commonly open because they are tied to internal services and hosts that are intended to be accessible to external hosts. These include the following:

- TCP 80 — HTTP web servers
- TCP 443 — HTTPS web servers
- TCP / UDP 53 — DNS servers
- TCP 25 and 587 — SMTP servers

An external network's attack surface increases with the number of open ports. Open ports should be limited to approved business use cases only. Here we focus on systems ports (those less than 1024).

Observed Activity

ThreatINSIGHT observed 14 open port(s) on the network perimeter, which were the destination port for at least one successful connection from an external host to an internal host. The top ten ports by number of connections are shown below and include the top three external sources of the connections.

Port	Description	Source Organizations	Connections
0	ICMP	Amazon.com, Inc. (US) Level 3 Parent, LLC (US) WZ Communications Inc. (US)	683,406 172,409 56,345
993	IMAP-SSL	Comcast Cable Communications, LLC (US) Frontier Communications of America, Inc. (US) Cellco Partnership DBA Verizon Wireless (US)	266,310 117,614 32,010
123	NTP	Comcast Cable Communications, LLC (US) Frontier Communications of America, Inc. (US) CenturyLink Communications, LLC (US)	79,768 33,885 3,652
[redacted]	SMTP-SSL	Rostelecom (RU) Bangalore Broadband Network Pvt Ltd (IN) Techcrea Solutions SARL (FR)	14,345 13,877 8,567
22	SSH	DigitalOcean, LLC (US) OVH SAS (CA) TierPoint, LLC (US)	5,585 1,637 716
[redacted]	[redacted]	Comcast Cable Communications, LLC (US) Frontier Communications of America, Inc. (US) DigitalOcean, LLC (US)	1,262 852 606
636	LDAP-SSL	TierPoint, LLC (US) DigitalOcean, LLC (US) M247 Ltd (US)	977 644 84
[redacted]	[redacted]	DigitalOcean, LLC (US) CONTINENTAL BROADBAND PENNSYLVANIA, INC. (US) Amazon.com, Inc. (US)	590 508 84
[redacted]	[redacted]	DigitalOcean, LLC (US) Merit Network Inc. (US) Capitalonline Data Service Co.,LTD (HK)	525 9 7

21	FTP	DigitalOcean, LLC (US) Hurricane Electric LLC (US) Merit Network Inc. (US)	99 30 28

Table 3: Top 10 Uncommon Open Ports by Number of Connections

Example IQL Query

```
src.internal = false AND src.asn.asn_org <> null AND dst.internal = true AND dst.port NOT IN (80,443,53,25,587) AND dst.port < 1024 AND flow_state NOT IN ('REJ','RSTOS0','SH') AND dst.ip_bytes > 0 GROUP BY dst.port LIMIT 100, src.asn.asn_org LIMIT 3
```

Recommended Remediation

Review the open ports and associated connections to ensure that the port is open for a legitimate business function and that the connecting source organization is authorized. Open ports that are not required for a legitimate business reason should be closed.

Connection Rejections [LOW]

Connection rejections are sent by devices, generally firewalls, to signal that an attempted connection is not allowed by the device's rule set. The benefit of returning a rejection to the requesting host is an expedient signal that the connection has failed. This generally improves the performance of the application responsible for the request as the application avoids waiting for its specified time-out period. Internal applications can benefit from this configuration, but it can hinder perimeter security as it provides an attacker a mechanism to map the perimeter of the network.

Observed Activity

ThreatINSIGHT observed 100+ port(s) returning external connection rejections. The top ten ports by number of connections are shown below.

Ports	Description	Connections
20	FTP-Data	34
21	FTP-Command	242
22	SSH	1,014
23	Telnet	6,814
25	SMTP	559,001
53	DNS	568
80	HTTP	11,607
81	HTTP-ALT	653
123	NTP	109
143	IMAP	29,927

Table 4: Top 10 Ports with Rejected Connections by Number of Connections

ThreatINSIGHT IQL Query

```
src.internal = false AND src.asn.asn_org <> null AND dst.internal = true AND flow_state = 'REJ' GROUP BY dst.port LIMIT 100
```

Recommended Remediation

Consider configuring external firewalls to DROP traffic that is not permitted, rather than returning a REJECT. Rules that are configured to return a REJECT should have a valid business justification.

Outbound Traffic

SSH Connections to External Hosts [MODERATE]

Secure Shell (SSH) was designed as a replacement for Telnet and is a cryptographic network protocol for operating network services securely over an unsecured network. SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login and remote command execution, however other network services can be secured with SSH. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2.

Attackers can use SSH tunnels to mask their activities as it creates an encrypted tunnel enabling unauthorized data movement, the ability to bypass firewall rules, and may allow access back into the network. Outbound SSH activity is common in many environments, but the use of this protocol needs to be mapped back to approved business activities to confirm legitimacy.

Observed Activity

ThreatINSIGHT observed 23 internal host(s) with outbound SSH sessions to external hosts. The top ten internal hosts by number of connections and the top three external connection sources per host are shown below.

Source Host	Target Organizations	Connections
[redacted]	Amazon.com, Inc. (US)	547
[redacted]	Amazon.com, Inc. (US)	469
[redacted]	Total Server Solutions L.L.C. (US) M247 Ltd (US) DigitalOcean, LLC (US)	151 26 11
[redacted]	Amazon.com, Inc. (US) Visionary Communications, Inc. (US) King County Library System (US)	126 6 4
[redacted]	Total Server Solutions L.L.C. (US) Linode, LLC (US) Hosting Services, Inc. (US)	76 45 8
[redacted]	Amazon.com, Inc. (US)	110
[redacted]	Total Server Solutions L.L.C. (US) Linode, LLC (US) DigitalOcean, LLC (US)	52 34 20
[redacted]	M247 Ltd (US) Linode, LLC (US) 1&1 Internet SE (GB)	47 30 19
[redacted]	Linode, LLC (US) M247 Ltd (US) DigitalOcean, LLC (US)	27 7 1
[redacted]	Linode, LLC (US) Total Server Solutions L.L.C. (US) M247 Ltd (US)	13 13 8

Table 5: Top 10 Hosts with outbound SSH connections by number of Connections

Example Query

```
src.internal = true AND dst.internal = false AND ssh:auth_success = true GROUP BY src.ip LIMIT 1000, dst.asn.asn_org LIMIT 3
```

Recommended Remediation

Review outbound SSH traffic for suspicious activity, or traffic that does not match approved business activities. Gigamon recommends creating a custom detection within the ThreatINSIGHT portal to monitor for outbound use of the SSH protocol, excluding any that is formally approved, to flag any potential malicious SSH connections.

IRC Connections to External Hosts [MODERATE]

Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in the form of text. The chat process works on a client/server networking model. IRC clients are computer programs that a user can install on their system or web-based applications running either locally in the browser or on 3rd party server. These clients communicate with chat servers to transfer messages to other clients. IRC is mainly designed for group communication in discussion forums, called channels, but also allows one-on-one communication via private messages as well as chat and data transfer, including file sharing[3].

Internet Relay Chat (IRC) activity introduces risk to the network by allowing outbound communication that may be unencrypted or expose a host's public IP address. Additionally, attackers can use IRC as an avenue for command and control (C2) traffic.

Observed Activity

ThreatINSIGHT observed 1 host(s) with outbound IRC traffic. The top ten internal hosts by number of connections and the top three external connection sources per host are shown below.

Source Host	Target Organizations	Connections
[redacted]	No.288,Fu-chun Road (CN)	1

Table 6: Top 10 Hosts with outbound IRC traffic by number of Connections

Example Query

```
src.internal = true AND dst.internal = false AND service = 'irc' GROUP BY src.ip LIMIT 1000, dst.asn.asn_org LIMIT 3
```

Recommended Remediation

Investigate all occurrences of IRC traffic within the network, disable it wherever possible, and block inbound IRC traffic from the internet.

[3] "Internet Relay Chat - Wikipedia." https://en.wikipedia.org/wiki/Internet_Relay_Chat. Accessed 15 May 2018.

Large Data Transfers to External Hosts [MODERATE]

Large movements of data to a host outside of the environment may represent risks to organizations including data theft or misuse of corporate resources. This metric utilizes a threshold of at least 1 GB of data leaving an internal host, with the external host responding with less than 500 MB of data, during a single connection which is indicative of a data upload.

Observed Activity

ThreatINSIGHT observed 75 host(s) transfer a total of 332.96 GBs to [LARGE_ORGS] organizations, collectively. The byte totals refer only to the sum of data transferred during connections that meet the specified threshold, and not all connections for the internal host(s). The top ten hosts by byte count and the top three external targets of the transfers per host are shown below.

Source Host	Target Organizations	Bytes (GB)
[redacted]	Oath Holdings Inc. (US)	35.18
[redacted]	Google LLC (US)	16.9
[redacted]	Amazon.com, Inc. (US)	14.18
[redacted]	Google LLC (US)	13.02
[redacted]	Apple Inc. (US)	11.91
[redacted]	Microsoft Corporation (US)	11.05
[redacted]	Google LLC (US)	10.96
[redacted]	Google LLC (US)	10.18
[redacted]	Microsoft Corporation (US)	9.94
[redacted]	Google LLC (US)	9.35

Table 7: Top 10 Hosts with large outbound transfers by total Bytes

Example Query

```
src.internal = true AND dst.internal = false AND proto = 'tcp' AND src.ip_bytes > 1000000000 AND dst.ip_bytes < 500000000 AND dst.asn.isp != 'Icebrg'
```

Recommended Remediation

Review the traffic and determine if a valid business justification exists. If so, ensure that appropriate controls exist to protect the data.

Third-Party Remote Access Utilities [MODERATE]

LogMeIn, TeamViewer, and other remote access applications enable complete remote control over hosts without requiring corporate authentication in any way. This software can enable remote access by both former employees, and malicious actors. Though not malicious in nature specifically, the existence of such software represents a security risk. Recent mass compromises of account details have enabled large scale comprises of users of TeamViewer and other remote desktop services.

Observed Activity

ThreatINSIGHT observed 11 host(s) utilizing remote access utilities. The top ten hosts by number of connections and the top three domains per host are shown below.

Source Host	Domains	HTTP Events
[redacted]	teamviewer.com logmein.com	21 9
[redacted]	teamviewer.com	12
[redacted]	teamviewer.com	9
[redacted]	teamviewer.com	3
[redacted]	teamviewer.com	3
[redacted]	teamviewer.com	2
[redacted]	teamviewer.com	2
[redacted]	teamviewer.com	2
[redacted]	teamviewer.com	1
[redacted]	logmein.com	1

Table 8: Top 10 Hosts communicating with third-party remote access services by number of Events

Example Query

```
http:host matches
'.*(gotomypc.com|logmein.com|bomgar.com|teamviewer.com|screenconnect.com|splashdot.com|realvnc.com|nomachine.com|anyplace-
control.com|remoteutilities.com|ammyy.com|join.me|beamyourscreen.com|uvnc.com|aeroadmin.com|remotepc.com|seescreen.com|anydesk.com|litemanager.com|comodo.com|showmypc.com).*' GROUP BY src.ip LIMIT 1000, http:host LIMIT 10
```

Recommended Remediation

Determine if activity is authorized according to internal policy. If not approved by corporate policy, remove remote access software.

Direct HTTP Traffic to External Hosts [LOW]

In organizations that have implemented HTTP proxies for filtering internet-bound traffic, direct HTTP identifies hosts which may have circumvented those proxies, exposing the environment to unnecessary risk and bypassing corporate policies. In organizations that utilize inline filtering for outbound traffic, direct HTTP traffic identifies systems which have made such outbound requests.

Observed Activity

ThreatINSIGHT observed 1,000+ host(s) with direct HTTP events. The top ten internal hosts by number of connections are shown below. The top results by count may represent corporate proxies. All others would represent workstations/other hosts with direct HTTP access externally.

Source Host	HTTP Events
[redacted]	149,692
[redacted]	72,141
[redacted]	66,458
[redacted]	54,262
[redacted]	53,063
[redacted]	52,743
[redacted]	52,504
[redacted]	49,442
[redacted]	48,666
[redacted]	45,378

Table 9: Top 10 Hosts with direct outbound HTTP traffic by number of Events

Example Query

```
src.internal = true AND dst.internal = false AND service = 'http' GROUP BY src.ip LIMIT 1000
```

Recommended Remediation

Validate that the listed systems represent the set of assets that can directly access Internet resources. Gigamon recommends the use of an outbound network traffic filter configured to block common threats to the environment, enforce corporate policies, and enable the information security team to block more advanced threats discovered during investigations.

Direct DNS Traffic to External Hosts [LOW]

Direct DNS traffic can allow rogue DNS servers to return incorrect IP addresses to DNS requests, therefore directing corporate systems to spoofed websites. Scammers utilize such attacks, known as “pharming”, to steal personal and corporate information.

Observed Activity

ThreatINSIGHT observed 1,000+ host(s) with direct DNS events to 100+ external DNS servers. The top 10 hosts for each metric by number of connections are shown below. The top results by count in the left table are likely corporate DNS servers. All other entries would represent workstations/other hosts with direct DNS access externally and the external DNS servers being used, respectively.

Source Host	DNS Events		Target Host	Organization	DNS Events
[redacted]	72,464,646		193.108.88.128	Akamai International B.V.	3,160,904
[redacted]	20,941,332		95.101.36.128	Akamai International B.V.	2,557,153
[redacted]	1,984,188		216.239.34.10	Google LLC	2,045,011
[redacted]	1,781,481		174.138.33.20	DigitalOcean, LLC	1,983,744
[redacted]	1,226,539		216.239.36.10	Google LLC	1,829,007
[redacted]	1,059,789		185.107.94.12	NForce Entertainment B.V.	1,282,193
[redacted]	883,801		8.8.8.8	Google LLC	1,034,786
[redacted]	856,905		13.107.252.10	Microsoft Corporation	1,030,717
[redacted]	765,145		165.227.241.122	DigitalOcean, LLC	967,452
[redacted]	764,023		205.251.198.22	Amazon.com, Inc.	828,087

Table 10: Top 10 Hosts with direct outbound DNS traffic and target hosts by number of Events

Example Query

```
src.internal = true AND dst.internal = false AND dst.asn.asn_org <> null AND dst.port = 53 GROUP BY src.ip LIMIT 1000
```

Recommended Remediation

Implement a centralized DNS server infrastructure that enforces internal clients to request DNS resolution through those servers only. Configure the internal DNS infrastructure to utilize only a small number of trusted external DNS servers, ideally with primary and secondary servers hosted by differing providers, only allowing the DNS infrastructure the ability to reach the trusted external servers directly.

Direct SMTP Traffic to External Hosts [LOW]

Clients should only send and receive email via approved SMTP servers. Allowing direct SMTP messages bypasses monitoring and increases the organization's risk of inclusion on spam blacklists, which can prevent the successful delivery of legitimate business email.

Observed Activity

ThreatINSIGHT observed 314 host(s) with direct SMTP events. The top ten hosts by number of connections are shown below. The top results by counts are likely corporate SMTP servers. All others would represent workstations/other hosts with direct SMTP access externally.

Source Host	SMTP Events
[redacted]	37,118
[redacted]	6,123
[redacted]	5,915
[redacted]	4,635
[redacted]	4,235
[redacted]	4,034
[redacted]	3,781
[redacted]	2,928
[redacted]	2,781
[redacted]	2,763

Table 11: Top 10 Hosts with direct outbound SMTP traffic by number of Events

Example Query

```
service = 'smtp' AND src.internal = true AND dst.internal = false AND dst.port = 25 GROUP BY src.ip LIMIT 1000
```

Recommended Remediation

Enforce all inbound and outbound SMTP traffic through corporate-hosted SMTP proxies, ideally with the ability to enforce detection and eradication of spam messages. Only these proxies should have the ability to communicate outbound over TCP port 25 to the internet.

Third-Party Data Storage Services [LOW]

DropBox, Google Drive, and other third-party data storage services enable the storage of sensitive organizational information outside the control of corporate policies. This leaves the organization vulnerable to insider threats, or data theft through the compromise of accounts or systems beyond the control of the organization.

Observed Activity

ThreatINSIGHT observed 124 host(s) utilizing third party data storage services. The top ten hosts by number of connections and the top three domains per host are shown below.

Source Host	Domains	HTTP Events
[redacted]	getdropbox.com	388
[redacted]	getdropbox.com	348
[redacted]	getdropbox.com	237
[redacted]	getdropbox.com	214
[redacted]	getdropbox.com	183
[redacted]	getdropbox.com	176
[redacted]	getdropbox.com	142
[redacted]	getdropbox.com	120
[redacted]	getdropbox.com	109
[redacted]	getdropbox.com	25

Table 12: Top 10 Hosts communicating with third-party data storage services by number of Events

Example Query

```
http:host matches
'.*(dropbox.com|\.box.com|idrive.com|sugarsync.com|onedrive.com|spideroak.com|certainsafe.com|onedrive.live.com|free-
hidrive.com|mega.nz|pcloud.com|mediafire.com|flipdrive.com|ozibox.com|disk.yANDex.com|\.sync.com|hubic.com|jumpshare.com|mydrive.ch|eyun.360.cn|mozy.com).*' GROUP BY src.ip LIMIT 1000, http:host LIMIT 10
```

Recommended Remediation

Determine if activity is authorized according to internal policy. If not approved by corporate policy, remove and block the infracting storage service.

Internal Traffic

End-of-Life (EOL) Windows Operating Systems [HIGH]

Microsoft does not continue to support patches for Windows systems indefinitely. Instead, they encourage customers to upgrade or migrate to newer versions. Legacy systems running older versions are at increased risk of compromise for security vulnerabilities discovered beyond the EOL date.

Observed Activity

ThreatINSIGHT observed 117 host(s) possibly utilizing EOL versions of Microsoft Windows. The operating system (OS) versions are fingerprinted using Windows kernel information observed in HTTP traffic. Windows kernel versions are generally tied to both a desktop and server version; for example, the Windows NT 6.1 is used by both Windows 7 and Windows Server 2008. In some cases, it may not be possible to distinguish between the desktop and server version, in which case both are listed. Additionally, some internal hosts identified may not be a desktop or workstation as some security appliances run outdated or embedded versions of Windows. The top ten hosts by number of connections and a breakdown of internal versus external connections per host are shown below.

Internal Host	OS Version	Internal Events	External Events
[redacted]	Windows XP Professional x64 / Server 2003	0	5,034
[redacted]	Windows XP	0	4,838
[redacted]	Windows XP	0	4,309
[redacted]	Windows XP	0	3,402
[redacted]	Windows XP Professional x64 / Server 2003	0	3,322
[redacted]	Windows XP	0	3,014
[redacted]	Windows XP	0	2,305
[redacted]	Windows XP	0	2,101
[redacted]	Windows XP	0	1,992
[redacted]	Windows XP Professional x64 / Server 2003	0	1,652

Table 13: Top 10 Hosts with EOL Windows software by number of Events

Example Query

```
src.internal = true AND (user_agent MATCHES '.*Windows[ /]{0,1}(NT (5|4)\.[0-9]|XP|200[03]).*' OR user_agent MATCHES 'Microsoft(-CryptoAPI/5| BITS/[0-6])\..*') GROUP BY src.ip LIMIT 1000, user_agent LIMIT 10
```

Recommended Remediation

Validate the presence of the described Windows versions within the environment. Wherever possible, update systems to the most recent version of the Windows operating system. In the case of business-critical systems that cannot be upgraded, segment these systems from the network, or completely disconnect them if possible. Any systems remaining on the network should also undergo frequent, recurring audits to validate additional controls remain in place.

Deprecated SSL Versions [HIGH]

The use of outdated SSL versions may enable an attacker to conduct man-in-the-middle attacks, or otherwise decrypt communications between the affected service and clients.

Observed Activity

ThreatINSIGHT observed 38 internal host(s) utilizing deprecated SSL for inbound communications. The top 10 hosts by number of connections are shown below; connections are split by whether they were internal or external to the network.

Target Host	SSL Versions	Internal Events	External Events
[redacted]	TLSv10	0	78,634
[redacted]	TLSv10	0	17,992
[redacted]	TLSv10, SSLv3	0	17,267
[redacted]	TLSv10, SSLv3	0	17,050
[redacted]	TLSv10	0	15,757
[redacted]	TLSv10	0	15,620
[redacted]	TLSv10	0	14,939
[redacted]	TLSv10	0	11,463
[redacted]	TLSv10	0	11,139
[redacted]	TLSv10	0	8,709

Table 14: Top 10 Hosts with outdated SSL software by number of Events

Example Query

```
ssl:version IN ('SSLv2', 'SSLv3', 'TLSv10') AND dst.internal = True GROUP BY dst.ip LIMIT 1000, ssl:version LIMIT 3
```

Recommended Remediation

Utilize up-to-date and properly configured encryption profiles on all web servers. Qualys has created and maintains thorough documentation[4] on the proper configuration of web server.

[4] "SSL and TLS Deployment Best Practices." https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices. Accessed 15 May 2018.

Outdated Browsers [MODERATE]

Outdated browsers may contain vulnerabilities that can be exploited by attackers using techniques such as cross-site scripting and cross-site request forgery.

Observed Activity

ThreatINSIGHT observed 1,000+ host(s) running outdated versions of five popular browsers:

- Microsoft Internet Explorer (MSIE)
- Chrome
- Firefox
- Safari
- Opera

The following table summarizes the distinct number of outdated major versions and the oldest major version observed in the environment for each browser. Note: hosts can have more than one outdated browser installed, so the sum of the Host Count column below will likely not match the figure above.

Browser	Host Count	Distinct Versions	Oldest Version
Chrome	1,000+	42	13
MSIE	205	6	5
Firefox	1,000+	36	3
Safari	1,000+	9	1
Opera	10	2	10

Table 15: Hosts with outdated browser software by number of Events

Example Query

```
(software:software_name = 'Chrome' AND software_version.major > 0 AND software:software_version.major < 66)OR (software:software_name = 'MSIE' AND software_version.major > 0 AND software_version.major < 11)OR (software:software_name = 'Firefox' AND software_version.major > 0 AND software_version.major < 58)OR (software:software_name = 'Safari' AND software_version.major > 0 AND software_version.major < 11)OR (software:software_name = 'Opera' AND software_version.major > 0 AND software:software_version.major < 49) GROUP BY host LIMIT 1000
```

Recommended Remediation

Perform patch management on all software in the environment, including browsers. In cases where browsers cannot be updated, isolate the host from the environment, allowing it access to only the specific resources required for business functionality.

Outdated Java [MODERATE]

Attackers frequently target vulnerable Java versions in exploitation attempts using exploit kits and drive by downloads. These exploits and payloads often result in additional malware being installed that could significantly impact the security of the system.

Observed Activity

ThreatINSIGHT observed 34 host(s) running 11 unique, outdated Java versions within the environment. [JAVA_MIN] was the oldest version observed. The top ten hosts by number of connections and top three Java versions per host are shown below.

Internal Host	Java Versions	HTTP Events
[redacted]	Java/1.6.0_45	1,112
[redacted]	Java/1.6.0_45	57
[redacted]	Java/1.7.0-u40	29
[redacted]	Java/11.0.2	11
[redacted]	Java/1.7.0-u40	8
[redacted]	Java/11.0.2	5
[redacted]	Java/1.7.0-u40	4
64.235.154.100	Java/1.7.0_76	4
[redacted]	Java/1.6.0_65	3
[redacted]	Java/1.7.0-u40	3

Table 16: Top 10 Hosts with outdated Java software by number of Events

Example Query

```
http:user_agent like 'Java/%' AND http:user_agent NOT like 'Java/THttp%' AND http:user_agent not like 'Java/1.8.0_%' AND http:user_agent!= 'Java/1.8.0_0-release' GROUP BY src.ip LIMIT 1000, http:user_agent LIMIT 5
```

Recommended Remediation

Perform patch management on all software in the environment, including Java. In cases where Java cannot be updated, isolate the host from the environment and only allow it access to the specific resources required for business functionality.

Appendices

Network Security Posture Details

Gigamon provided the external document “Northshore School District - Network Security Posture Report - Detailed Data Listing.xlsx”, which contains detailed information[5] on Network Security Posture queries that returned more than ten hosts.

Asset Inventory

Gigamon provided an inventory of assets observed in the network in the external document “Northshore School District - Asset Inventory.xlsx”, which was generated from DHCP leases, passive DNS, and Kerberos client requests.

[5] Note that results are limited to the top 10,000 results. Full results are available through the ICEBRG portal.