



《o》 Muninn

2022

Network Encryption Threat Report



TABLE OF CONTENTS

2_ Introduction

3_ Half-year 2022 Notification Trends.

4_ Technical Deep Dive: *Vulnerable External SSL Connection*

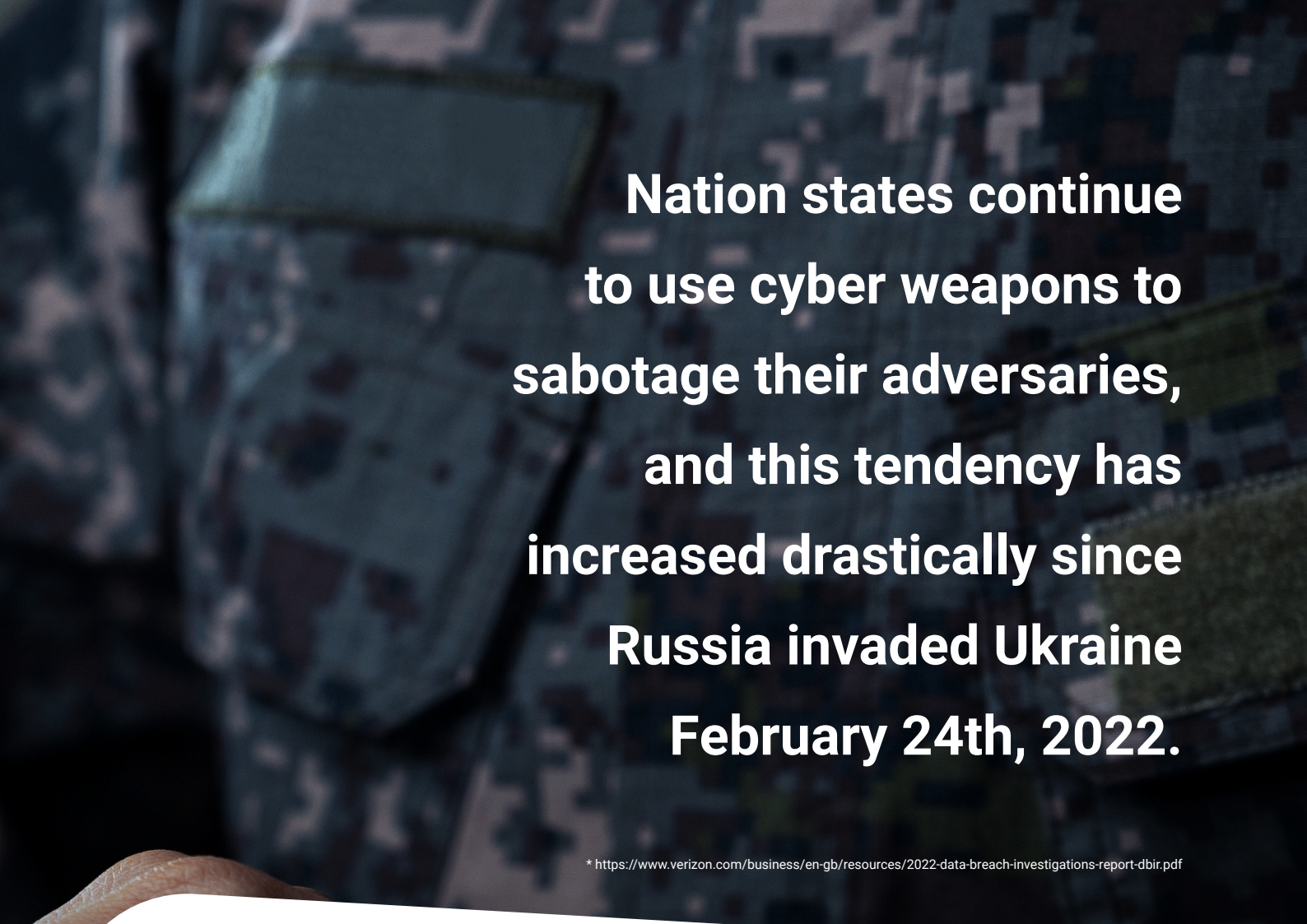
6_ What is Important to Secure SLL and TSL Connections: *Checklist*

7_ Identify Vulnerable Connections: *Monitoring*

9_ Expired SSL Certificate from External Server: *In-Depth Analysis*

11_ Insights from Muninn: *In Prattice*

12_ About us



**Nation states continue
to use cyber weapons to
sabotage their adversaries,
and this tendency has
increased drastically since
Russia invaded Ukraine
February 24th, 2022.**

* <https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf>

Introduction

Cybersecurity has been a growing concern for corporations, governments, and individuals over the past decade or more. According to the Verizon 2022 Data Breach Investigations Report*, **83%** of Organizations had more than one data breach in 2022 and on average organizations experienced **28+** attacks. The use of cyberweapons by nation-states to undermine their rivals has surged, particularly since Russia's invasion of Ukraine in February 2022.

In Muninn's Threat Report, we will dive into the diverse range of cyberattacks that Muninn's global sensor network has detected in the aftermath of Russia's military actions in Ukraine.

Identifying the perpetrators behind cyberattacks is a complex task, especially when the attacks are orchestrated by state-sponsored cybercriminal groups. Nonetheless, we have seen a noticeable uptick in alerts originating from Russian or Belarusian IP addresses since the onset of the Ukrainian conflict.

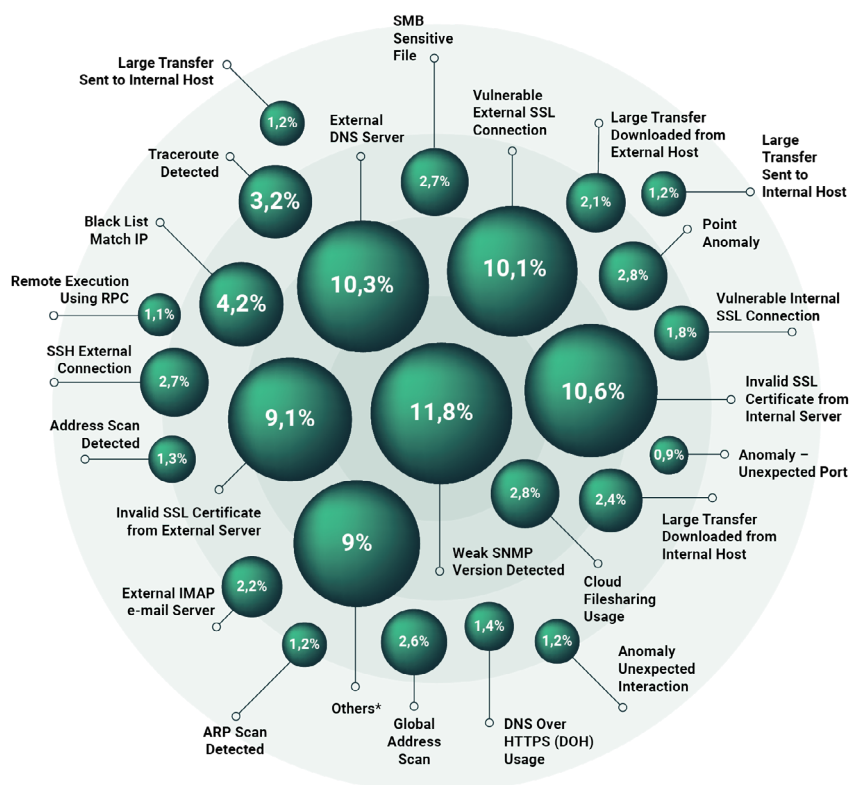
For the first half of 2022, Muninn's network sensors have processed and analyzed vast volumes of global network data, generating threat alerts that have enabled numerous companies to sidestep significant cybersecurity incidents.

The subsequent section offers a comprehensive statistical analysis, detailing the variety and volume of threats that Muninn's sensors have identified across our entire client base.

Top 50 Notifications in H1 2022

*Under 1%

Lateral movement using SMB admin shares
 Selective Port Scan
 Soon to expire SSL certificate from internal server
 Expired SSL certificate from internal server
 OT unknown function codes
 Anomaly - Unexpected Service
 External SMTP e-mail server
 Port scan detected
 SSH Interesting Hostname Login
 RDP Outgoing Connection
 Expired SSL certificate from external server
 Tor middle node communication
 Exfiltration of many files
 HTTP SQL injection detected
 Blacklist match file Anomaly - Data Transfer
 External POP3 e-mail server
 SSH Failed Attempts
 Soon to expire SSL certificate from external server
 DNS Multiple Domain Not Found
 Anomaly - Out of hours
 Tor exit node connection
 Misconfigured HTTP basic auth client
 Anomaly - Unexpected Service and Port
 Blacklist match certificate
 P2P traffic patterns
 Kerberos Longlived Ticket
 HTTP SQL injection victim detected
 Secure com password guessing attempts detected
 DNS over HTTPS (DOH) usage
 HTTP crawler detected
 SMB Suspicious File Renaming
 Event log clearing or forced reboot using RPC
 DNS Tunneling
 Impossible travel detected
 Login from an unprecedented country
 Anomaly - Unusual Context
 Global port scan
 Reverse SSH
 Large amount of files downloaded
 FTP brute force login detected
 DarkNet or Tor activity detected
 Local blacklisted executable detected
 Not yet valid SSL certificate from internal server
 HTTP Authentication Bruteforce
 Lateral movement and execution
 Too many failed login attempts for user
 Too many failed login attempts from IP
 Blacklist match SSH
 BitTorrent port usage
 Crypto Currencies Mining Pool Activity
 Large amount of mail attachment sent
 Login from an unexpected country
 NTLM User Password Bruteforce
 Failed login attempt from an unprecedented country
 Blacklist match domain
 SMB Ransomware filename detected



Notification Trends H1 2022

In the first half of 2022, Muninn's sensors observed a notable uptick in the detection of "Weak SNMP versions," accounting for 11.8% of all notifications. For a detailed technical breakdown of this category, read our annual report. On the other hand, "Vulnerable external SSL connections" were slightly less common in the first quarter of 2022, making up 14.6% of all notifications. This is a decrease compared to the same period in 2021, where they constituted 10.9% of all notifications. A comprehensive technical explanation for this category will be provided in a later section of this report. Similarly, "Invalid SSL certificates

from internal servers" saw a minor increase in the first half of 2021, comprising 8.9% of all notifications, compared to the full year of 2021. The frequency of notifications for "External DNS servers" has declined to 10.3%. In the first half of 2022, "Vulnerable external SSL connections" were less frequent, making up 10.1% of all notifications, a decrease from the previous year. Additionally, the category 'Invalid SSL certificate from external server' dropped to 9.1%. Technical explanations for both "Vulnerable external SSL connections" and "Expired SSL certificate from external server" will be covered in a subsequent section of this report.



Technical Deep Dive

Vulnerable External SSL Connection

Henrik Falkenthros Senior IT Security Engineer



Threat Identification

Muninn is engineered to pinpoint weak encryption protocols in order to safeguard data as it moves across networks. Specifically, it scans for vulnerable or unencrypted SSL connections within network traffic. This enables security managers to proactively address network vulnerabilities.

Exploitation Methods

SSL and TLS protocols have long been a focal point for various types of cyberattacks. One common

method employed by threat actors is the "Man-in-the-Middle" attack, which allows unauthorized access to encrypted communications. Other prevalent techniques include protocol downgrading, stripping, and memory reading.

Attack Vectors

A multitude of strategies exist for exploiting vulnerable SSL connections. A quick Google search using terms like FREAK, DROWN, SWEET32, HeartBleed, POODLE, BREACH, and CRIME will provide ample information. Instructions for executing

Man-in-the-Middle attacks are readily available online, with GitHub hosting several relevant repositories. Typically, attackers aim for the network's weakest link, provided that the target holds sufficient value or interest.

```
Terminal
sirhenry@192.168.2.126: ~/Documents/Godfathers/lp-map/lpranges
$sslsan samplelabserver.com
Version: 2.6.7
OpenSSL 1.1.1f 31 Mar 2020

Connected to 186.2.109.7

Testing SSL server samplelabserver.com on port 443 using SNI name samplelabserver.com

SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 enabled
TLSv1.1 enabled
TLSv1.2 enabled
TLSv1.3 disabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Secure session renegotiation supported

TLS Compression:
OpenSSL version does not support compression
Rebuild with zlib-dev package for zlib support

Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-384 DHE 384
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-384 DHE 384
Accepted TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
Accepted TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-384 DHE 384
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-384 DHE 384
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve P-384 DHE 384
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-384 DHE 384
Accepted TLSv1.2 128 bits DHE-RSA-AES128-SHA256 DHE 2048 bits
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 2048 bits
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA DHE 2048 bits
Accepted TLSv1.2 128 bits AES128-GCM-SHA256
Accepted TLSv1.2 256 bits AES256-GCM-SHA384
Accepted TLSv1.2 128 bits AES128-SHA256
Accepted TLSv1.2 256 bits AES256-SHA256
Accepted TLSv1.2 128 bits AES128-SHA
Accepted TLSv1.2 256 bits AES256-SHA
Accepted TLSv1.2 112 bits TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.2 112 bits TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.2 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
Preferred TLSv1.1 128 bits ECDHE-RSA-AES128-SHA Curve P-384 DHE 384
Accepted TLSv1.1 256 bits ECDHE-RSA-AES256-SHA Curve P-384 DHE 384
Accepted TLSv1.1 128 bits DHE-RSA-AES128-SHA DHE 2048 bits
Accepted TLSv1.1 256 bits DHE-RSA-AES256-SHA DHE 2048 bits
Accepted TLSv1.1 128 bits AES128-SHA
Accepted TLSv1.1 256 bits AES256-SHA
Accepted TLSv1.1 112 bits TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.1 112 bits TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.1 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
Preferred TLSv1.0 128 bits ECDHE-RSA-AES128-SHA Curve P-384 DHE 384
Accepted TLSv1.0 256 bits ECDHE-RSA-AES256-SHA Curve P-384 DHE 384
Accepted TLSv1.0 128 bits DHE-RSA-AES128-SHA DHE 2048 bits
Accepted TLSv1.0 256 bits DHE-RSA-AES256-SHA DHE 2048 bits
Accepted TLSv1.0 128 bits AES128-SHA
Accepted TLSv1.0 256 bits AES256-SHA
Accepted TLSv1.0 112 bits TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.0 112 bits TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.0 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA

Server Key Exchange Group(s):
TLSv1.2 192 bits secp384r1 (NIST P-384)

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject:
AltNames:
Issuer:

Not valid before: Feb 10 00:00:00 2018 GMT
Not valid after: Feb 10 23:59:59 2019 GMT

sirhenry@192.168.2.126: ~/Documents/Godfathers/lp-map/lpranges
$
```

In Practice

Case:

For illustrative purposes, let's consider <https://samplelabserver.com> as a hypothetical target.

Using a Kali Box, you can assess the security of the web server you wish to interact with by running a SSL scan command.

On the next page you will find eight important sections you should have a closer look at.

Checklist

What is Important to Secure SLL and TSL Connections

1. SSL/TLS Protocols

Both SSLv2 and v3 are disabled, which is a positive step as it prevents the use of these weaker encryption protocols between the client and the web server. However, it's concerning that TLSv1.0 and v1.1 are still supported, given their known vulnerabilities. Most notably, TLSv3 is disabled, which is surprising since it's widely regarded as the gold standard for secure network encryption.

2. TLS Fallback SCSV

The TLS Signaling Cipher Suite Value (SCSV) serves as a safeguard against downgrade attacks. When enabled, it ensures that the most robust protocol supported by both the client and server is utilized. It will also be an indicator that everything is in order as this feature is activated.

3. TLS Renegotiation

The web server allows for secure fallback, enabling the addition of authentication details to an existing connection when necessary aim for the network's weakest link, provided that the target holds sufficient value or interest.

4. TLS Compression

During the TLS Handshake process, options for data compression methods are negotiated. It's worth noting that sslscan doesn't check for this feature, so you should use nmap for verification:

```
nmap -sV --script ssl-enum-ciphers -p 443 samplelabserver.com
```

The shown nmap output indicates that no compression is being used. Additionally, the script checks for known vulnerabilities, such as SWEET32.

5. Heartbleed

The web server is not susceptible to Heartbleed, a well-known memory leak flaw in OpenSSL.

Verify using nmap:

```
nmap -d --script ssl-heartbleed --script-args vulns.showall -sV samplelabserver.com
```

The output stating 'ssl-heartbleed: NOT VULNERABLE' confirms the web server is not vulnerable.

6. Supported Server Ciphers

Cipher suites consist of various algorithms designed to secure SSL or TLS network connections. Typically, a cipher suite will include a key exchange algorithm, a bulk encryption algorithm, and a message authentication code (MAC) algorithm. Ciphers highlighted in green are secure and recommended for use, while those in white and orange are weak and should be avoided. For further details on cipher suites, you can visit <https://www.iana.org/>

7. Server Key Exchange Group

The elliptic curve P-384 offers a 192-bit security level and is employed for digital signatures and key-agreement protocols.

8. SSL Certificate Details

The signature algorithm used is sha256WithRSAEncryption, which signifies the hash algorithm employed to sign the SSL certificate. The RSA Key Strength stands at 2048, which is generally considered sufficient. However, it's important to note that the certificate is no longer valid.



Monitoring Identify Vulnerable Connections

Summary and Security Implications

After reviewing these eight key areas, there are multiple red flags that make connecting to this website a big mistake. The primary concerns include an expired SSL certificate, support for the outdated TLSv1.0, and the absence of support for TLSv3.

Hacker's Perspective

From an attacker's standpoint, the website's support for the weak TLSv1.0 protocol, with a 112-bit length and the inclusion of triple DES and CBC, presents a clear attack vector.

To confirm this, a hacker would execute the following Nmap command:

```
nmap -Pn --script ssl-enum-ciphers -p 443  
samplelabserver.com
```

For a hands-on, simplified example of executing a SWEET32 attack, you can refer to this repository: <https://github.com/azeemba/sour16>

According to databases like the National Vulnerability Database (NVD: <https://nvd.nist.gov/general/nvd-dashboard>), there have been over 10 new CVEs (Common Vulnerabilities and Exposures) related to SSL/TLS breaches recorded in 2022 alone. Since the inception of these records in 1999, the total number exceeds 3,500. Severity ratings often range from a CVSSv2 score of around 5.0 (medium) to 10.0 (high). Given that these vulnerabilities pertain to network security protocols, the high severity ratings are hardly surprising.

Muninn's Findings

Muninn AI Detect is engineered to detect vulnerable SSL connections, whether they are within the Local Area Network (LAN) or external. By scrutinizing the initial Ethernet frames, we can discern the type of network encryption negotiated between the client and the web server. This information is crucial for understanding the security level of the ensuing HTTPS session.

Data Extraction and TLS Handshake

The initial data packets serve as a valuable source for extracting information about an encrypted communication session. They can reveal key details such as HTTP URLs, DNS hostnames/addresses, and more. The TLS handshake process itself consists of multiple messages that contain unencrypted but significant metadata, including cipher suites, TLS versions, and the length of the client's public key.

Example Notification and Security Concerns

In the following section, you'll find an example notification triggered due to the use of the outdated TLSv1.0 protocol.

SSL and TLS protocols have long been susceptible to various forms of cyberattacks. Threat actors frequently employ "Man-in-the-Middle" attacks to gain unauthorized access to encrypted communications. Other common tactics include protocol bypassing, downgrading, stripping, and memory reading, all of which serve as potential attack vectors.

Muninn AI Detect is designed to catch communication with vulnerable SSL connections to web servers inside the LAN or to external. By analyzing the initial ethernet frames, we can see from the handshakes what type of network encryption is negotiated between client and webserver and thus to be used in the HTTPS session.

Notification Details

Short Description	Severity Level	Score	Time	Source	Target	Category	Source Type	Description	Action
Weak TLSv10 connection established between a local host and xdevice.ru	Low		03/29/2022 11:20:14 AM	10.11.11.137	xdevice.ru	Vulnerable external	Device	Weak TLSv10 connection established between a local host and xdevice.ru. Based on analysis event 29/2022 11:20:13 AM and a duration of N/A	[Icon]

No fetch has been initiated
You could try a meta data search instead by using the "Search More" action.

Q Search notifications

From: 01/01/2022 8:05 AM To: 05/06/2022 9:05 AM Host: 10.11.11.137 Severity: All

Found 7 matching results (max 1000)

Time	Host source	Destination	Severity
03/29/2022 11:20:14 AM	10.11.11.137	90.156.141.249	Low
03/29/2022 11:20:55 AM	10.11.11.137	90.156.141.249	Low
03/30/2022 12:42:23 PM	10.11.11.137	90.156.141.249	Low
03/30/2022 7:47:01 PM	10.11.11.137	90.156.141.249	Low
03/31/2022 6:49:02 AM	10.11.11.137	90.156.141.249	Low
04/11/2022 5:35:08 PM	10.11.11.137	90.156.141.249	Low
04/11/2022 6:10:19 PM	10.11.11.137	90.156.141.249	Low

Host information

IP: 90.156.141.249
MAC: Not Available
Hostname: Not Available
Domain: xdevice.ru
Country: RU
ASN: 25532 / LLC masterhost
Host Type: Unknown
OS: Unknown
First Seen: 03/29/2022 11:20:00 AM
Last Seen: 04/11/2022 5:35:00 PM
VLAN:
Users:

Category	Description	Action
Weak TLSv10 connection	Weak TLSv10 connection established between a local host and xdevice.ru	[Icon]
Weak TLSv10 connection	Weak TLSv10 connection established between a local host and xdevice.ru	[Icon]
Weak TLSv10 connection	Weak TLSv10 connection established between a local host and xdevice.ru	[Icon]
Weak TLSv10 connection	Weak TLSv10 connection established between a local host and xdevice.ru	[Icon]
Vulnerable external SSL connection	Weak TLSv10 connection established between a local host and xdevice.ru	[Icon]
Vulnerable external SSL connection	Weak TLSv10 connection established between a local host and xdevice.ru	[Icon]
Vulnerable external SSL connection	Weak TLSv10 connection established between a local host and xdevice.ru	[Icon]

Searching the metadata reveals the cipher suite used in the communication, **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA**:

Q Search Data

Meta Data Raw Data Audit Logs

4 hits on 10.11.11.137, port: any, from: 03/29/2022 11:15:53 AM, to: 03/29/2022 11:21:53 AM, type: any

Host: 10.11.11.137 Port: 443 From: 90.156.141.249 To: 10.11.11.137 Type: ssl

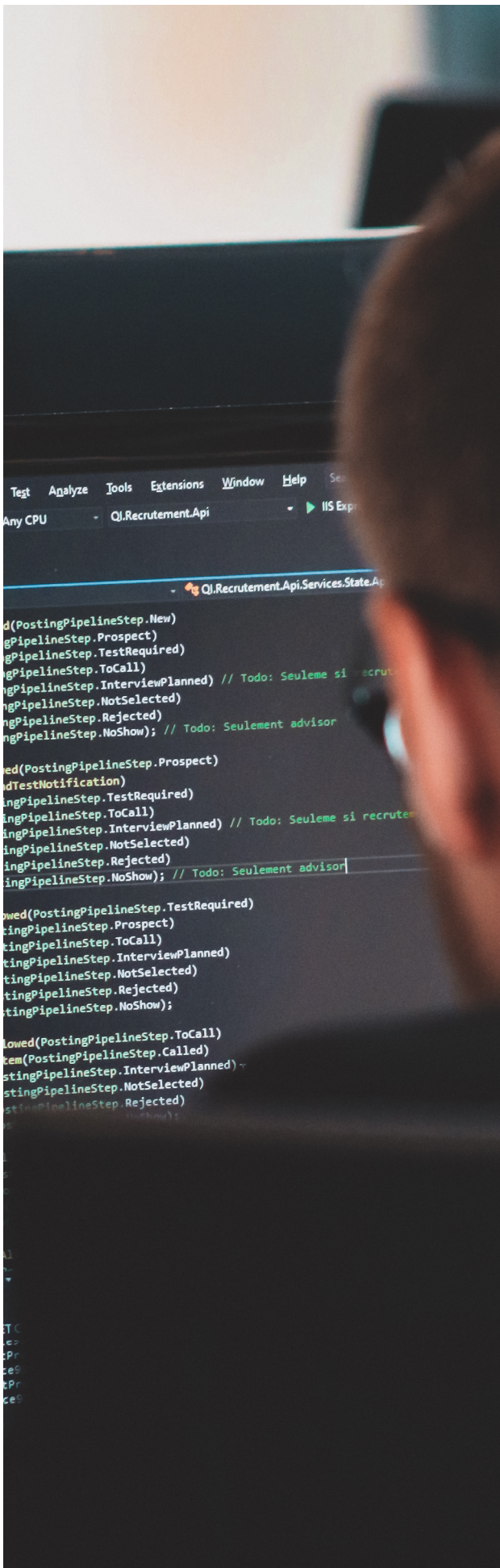
Advanced search

Use Connection Closing Time Search Archived Events Search for Process Names

Found 4 matching results (max 1000) in 104 ms.
Filtered statistics: Showing 4 of 4 events. Time span from 03/29/2022 11:20:13 AM to 03/29/2022 11:20:53 AM. Total connections: 2 with 0/05 connections per second, sent 2.3 Kib, received: 68.6 Kib.

Time	Type	Source	Target	Description	Description Details
03/29/2022 11:20:53 AM	ssl	10.11.11.137	90.156.141.249	xdevice.ru Port:443 TLSv10	cipher = TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, established = T, server_name = xdevice.ru, id.orig_p = 44900, id.vlan = 30, resp_ip_bytes = 35137, id.vlan = 30, id.orig_p = 443, id.vlan = 30, resp_ip_bytes = 1076, orig_pkts = 32, missed_bytes = 14794, history = SHA256GPTunnel, parents = duration = 0.241560, local_resp = Field = Ceyec03RqGUVLDj, client_subject = client, issuer = id.orig_p = 10.11.11.137, just_alert = validation_status = ok, resumed = F, id.orig_p = 90.156.141.249
03/29/2022 11:20:53 AM	conn	10.11.11.137	90.156.141.249	Ports 44900 -> 443 Sent/rcv 1076 -> 35137 bytes	id.orig_p = 44900, resp_pkts = 30, resp_ip_bytes = 35137, id.vlan = 30, id.orig_p = 443, id.vlan = 30, resp_ip_bytes = 1076, orig_pkts = 32, missed_bytes = 14794, history = SHA256GPTunnel, parents = duration = 0.241560, local_resp = Field = Ceyec03RqGUVLDj, client_subject = client, issuer = id.orig_p = 10.11.11.137, just_alert = validation_status = ok, resumed = F, id.orig_p = 90.156.141.249
03/29/2022 11:20:13 AM	ssl	10.11.11.137	90.156.141.249	xdevice.ru Port:443 TLSv10	cipher = TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, established = T, server_name = xdevice.ru, id.orig_p = 44896, id.vlan = 30, resp_ip_bytes = 35137, id.vlan = 30, id.orig_p = 443, id.vlan = 30, resp_ip_bytes = 1076, orig_pkts = 32, missed_bytes = 14794, history = SHA256GPTunnel, parents = duration = 0.240442, local_resp = Field = CAVVbKqUJZOT4t, client_subject = client, issuer = id.orig_p = 10.11.11.137, just_alert = validation_status = ok, resumed = F, id.orig_p = 90.156.141.249
03/29/2022 11:20:13 AM	conn	10.11.11.137	90.156.141.249	Ports 44896 -> 443 Sent/rcv 1232 -> 35137 bytes	id.orig_p = 44896, resp_pkts = 30, resp_ip_bytes = 35137, id.vlan = 30, id.orig_p = 443, id.vlan = 30, resp_ip_bytes = 1076, orig_pkts = 32, missed_bytes = 14794, history = SHA256GPTunnel, parents = duration = 0.240442, local_resp = Field = CAVVbKqUJZOT4t, client_subject = client, issuer = id.orig_p = 10.11.11.137, just_alert = validation_status = ok, resumed = F, id.orig_p = 90.156.141.249

Countermeasures Support only TLSv1.3 and above.



In-Depth Analysis Expired SSL Certificate from External Server

Henrik Falkenthros

Senior IT Security Engineer



The Threat

SSL certificates serve dual purposes: they authenticate the server and encrypt the data being transmitted. When a certificate expires, it compromises the server's authenticity, leaving users without the assurance that they are communicating with the intended server. This is because a Certificate Authority (CA) only issues a certificate after verifying the server owner's identity.

A malicious website won't possess the private key associated with the original certificate, which remains exclusive to the authentic server.

If you encounter an expired certificate, your browser will display multiple warning messages, indicating that the server is no longer trustworthy. While this is concerning, it's worth noting that the encryption level remains unchanged post-expiration.

For public-facing websites, these warnings can sow doubt among users and may deter them from engaging in online transactions.

The Exploitation

Cybercriminals often maintain extensive lists of companies, monitoring them for certificate expiration dates. Through Open Source Intelligence (OSINT) gathering, they create counterfeit websites that mimic the target company's branding. They also prepare a list of potential victims and secure a convincing domain name, for example 'verification-company.com,' complete with a valid SSL certificate.

Once the target company's certificate expires, the attackers initiate their phishing campaign. They send emails to the company's customers, urging them to "verify their accounts" on the newly-created fraudulent website. Unfortunately, only a small fraction of users will scrutinize the certificate details before entering their credentials, becoming a victim to the scam.

For instance, attackers might use Google hacking techniques to identify potential targets in various sectors like retail and fashion, compiling lists such as 'top-50-shops.lst' for future attacks.

Understanding these risks and attack vectors associated with expired SSL certificates enables both organizations and individual users to take preemptive steps to safeguard themselves.

For those with technical skills, you can download a script from GitHub or similar repositories that checks for certificate expiration. <https://github.com/codebox/https-certificate-expiry-checker/blob/main/check-certificates.py>

```
Clear; while read -r line; do sudo timeout 5 python3 check_certificates.py $line | awk '{print $1 "\t" "expires in "$5" "$6}'; done < top-50-shops.lst
```

Running a one-liner command in Kali Linux will show the necessary information.

Alibaba.com	expires in 261 days	hepsiburada.com	expires in 316 days
aliexpress.com	expires in 353 days	lkea.com	expires in 107 days
allegro.pl	expires in 72 days	Inditex.com	expires in 317 days
amazon.ca	expires in 321 days	jd.com	expires in 137 days
Amazon.co.jp	expires in 82 days	johnlewis.com	expires in 27 days
Amazon.co.uk	expires in 82 days	kakaku.com	expires in 124 days
Amazon.com	expires in 82 days	leboncoin.fr	expires in 267 days
amazon.com.br	expires in 310 days	lego.com	expires in 83 days
amazon.com.mx	expires in 319 days	mercadolibre.com.ar	expires in 247 days
Amazon.de	expires in 82 days	mercadolibre.com.mx	expires in 257 days
amazon.es	expires in 330 days	mercadolive.com.br	expires in 248 days
amazon.fr	expires in 319 days	mercari.com	expires in 209 days
Amazon.in	expires in 325 days	olx.com.br	expires in 316 days
amazon.it	expires in 328 days	olx.pl	expires in 231 days
americanas.com.br	expires in 239 days	ottogroup.com	expires in 377 days
Apple.com	expires in 331 days	ozon.ru	expires in 279 days
bestbuy.com	expires in 204 days	pinduoduo.com	expires in 275 days
Bol.com	expires in 152 days	rakuten.co.jp	expires in 142 days
Carrefour.com	expires in 171 days	sahibinden.com	expires in 293 days
Ceconomy.de	expires in 83 days	Shop.com	expires in 39 days
costco.com	expires in 310 days	shopee.co.id	expires in 127 days
craigslist.org	expires in 240 days	shopping.yahoo.co.jp	expires in 345 days
e.leclerc	expires in 114 days	taobao.com	expires in 110 days
ebay-kleinanzeigen.de	expires in 111 days	Target.com	expires in 123 days
Ebay.co.uk	expires in 213 days	Tesco.com	expires in 50 days
Ebay.com	expires in 213 days	ticketmaster.com	expires in 353 days
ebay.de	expires in 213 days	tokopedia.com	expires in 82 days
ecco.com	expires in 158 days	trendyol.com	expires in 327 days
etsy.com	expires in 262 days	Veepee.fr	expires in 199 days
Flipkart.com	expires in 23 days	walmart.com	expires in 305 days
groupe-casino.fr	expires in 128 days	wayfair.com	expires in 88 days
Groupon.com	expires in 225 days	Zalando.com	expires in 140 days

Crafting a Phishing Campaign: A Cautionary Note

While it's relatively straightforward to find email accounts associated with a specific domain like LEGO.com and craft a convincing phishing email, we strongly discourage engaging in such activities. Various methods exist for obtaining users' email addresses tied to a company, especially those with an online store. It is relatively easy to find full names and email addresses in numerous blogs where people discuss the company's products or services.

Social media platforms like Facebook, Twitter, and LinkedIn are also rich sources of information for understanding product or service interests. If one is not up for doing it, darknet services provide this information for a small fee. Which means even with a small amount of resources one can get a large amount of private information.\$

In Practice

Insights from Muninn

Muninn AI Detect is designed to trigger an alert based on the 'NotValidAfter' value of the SSL certificate.

Notification Details

Short Description	Severity Level	Score	Time	Source	Target	Category	Source Type	Description	Action
Certificate CN="*.torshavn.fo expired at 2021-06-17-12:00:00.000000000	Low		06/03/2022 4:07:10 AM	45.33.65.249 - Linode, LLC	azenv.net	Expired SSL certificate from external server	Device	Certificate CN="*.torshavn.fo expired at 2021-06-17-12:00:00.000000000 - Based on analysis event 06/03/2022 4:07:07 AM and a duration of N/A secs.	

No fetch has been initiated

You could try a meta data search instead by using the "Search More" action.

Q Search notifications

From To Host Severity Category Ack State Description

Found 164 matching results (max 1000)

Time	Host source	Destination	Severity	All Prevent Triggered	Score	Ack State	Category	Description	Action
			All						
06/03/2022 4:07:10 AM	45.33.65.249	192.168.1.10	Low	No		Unacknowledged	Expired SSL certificate from external server	Certificate CN="*.torshavn.fo expired at 2021-06-17-12:00:00.000000000 -	
06/03/2022 4:07:12 AM	45.33.65.249	192.168.1.10	Low	No		Unacknowledged	Expired SSL certificate from external server	Certificate CN="*.torshavn.fo expired at 2021-06-17-12:00:00.000000000 -	
06/04/2022 4:17:08 AM	162.142.125.7	192.168.1.10	Low	No		Unacknowledged	Expired SSL certificate from external server	Certificate CN="*.torshavn.fo expired at 2021-06-17-12:00:00.000000000 -	
06/04/2022 4:50:53 AM	205.210.31.144	192.168.1.10	Low	No		Unacknowledged	Expired SSL certificate from external server	Certificate CN="*.torshavn.fo expired at 2021-06-17-12:00:00.000000000 -	
06/04/2022 5:19:06 AM	128.14.141.34	192.168.1.10	Low	No		Unacknowledged	Expired SSL certificate from external server	Certificate CN="*.torshavn.fo expired at 2021-06-17-12:00:00.000000000 -	
06/04/2022 7:07:37 AM	170.187.203.244	192.168.1.10	Low	No		Unacknowledged	Expired SSL certificate from external server	Certificate CN="*.torshavn.fo expired at 2021-06-17-12:00:00.000000000 -	
06/04/2022 8:10:30 AM	35.81.79.158	192.168.1.10	Low	No		Unacknowledged	Expired SSL certificate from external server	Certificate CN="*.torshavn.fo expired at 2021-06-17-12:00:00.000000000 -	

Countermeasures

Avoid Communication:

Do not interact with servers or services that cannot present a valid SSL certificate.

Firewall Blocking:

If you determine that a website is malicious, permanently block its domain in your firewall.

Temporary Measures:

For websites that are generally trustworthy but have an expired SSL certificate, consider temporarily blocking the domain in your firewall. Additionally, notify your external partners that they are operating with expired certificates.

During their Open Source Intelligence (OSINT) data collection, hackers construct counterfeit websites that closely mimic the target's visual branding. They also compile a list of users to target for their attacks. To lend credibility to their fraudulent sites, they acquire convincing domain names, such as 'verification-company.com,' along with valid SSL certificates.

About us

Founded in 2016 by engineers and computer scientists from the prestigious Massachusetts Institute of Technology (M.I.T), Muninn has been changing the way companies approach cybersecurity. With our advanced AI technology and reliable security solutions, Muninn AI Detect and AI Prevent empower organizations to protect their critical digital assets and infrastructures from cybercriminals.

Located in the heart of Denmark, in Copenhagen, our team is comprised of inspiring colleagues with multiple nationalities and backgrounds. Each employee is committed to professional development and growth, ensuring that Muninn will continue to be a game-changer in the field of cybersecurity.

Named after one of Odin's ravens, Muninn, we are innovative and curious: about our customers, their challenges, trends that shape the future of the digital landscape and groundbreaking solutions that will bring cybersecurity to a new level. You can call us "geeks", if you like, because we are passionate about every single detail that make our technology so great.



References

- <https://sweet32.info/>
- <https://heartbleed.com/>
- <https://www.exploit-db.com/>
- <https://www.keylength.com/en/4/>
- <https://nmap.org/book/man-nse.html>
- <https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml>
- <https://commandlinefanatic.com/cgi-bin/showarticle.cgi?article=art060>
- <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-186-draft.pdf>
- https://www.researchgate.net/publication/322056853_Speeding_up_Elliptic_Curve_Cryptography_on_the_P-384_Curve
- https://nvd.nist.gov/vuln/search/results?results_type=overview&query=ssl&search_type=all&form_type=Basic&isCpeNameSearch=false&orderBy=publishDate&orderDir=desc
- <https://github.com/azeemba/sour16/blob/master/-practical-kali-demo-of-cracking-encryption>
- <https://ciphersuite.info/search/?security=all> - secure cipher suites
- https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
- <https://docs.microsoft.com/en-us/windows/win32/seccertenroll/about-x-509-public-key-certificates>
- <https://gbhackers.com/latest-google-dorks-list/>



www.muninn.ai

info@muninn.ai

+45 70 60 59 08

Copyright © 2023

by Muninn