Arctic Security

Arctic EWS

Performance and Progression Report

ACME INC.

October 2022

contact@arcticsecurity.com https://arcticsecurity.com

EWS October 2022 in Numbers

Collected Observations	0
Tracked Malware Families	172
Tracked Vulnerabilities	113
Tracked Open Services	17

Your Configured Assets

IP Addresses and Networks	1
Domain Names	2
Enumerated Domain Names	50
Resolved IP Addresses	62

Arctic EWS helps you with **attack surface discovery** by automatically locating assets based on your domain names. This allows external **monitoring of vendor hosted assets** as well as those hosted by yourself.

Monthly Unique Issues for Acme Inc.

SEVERITY	2022-05	2022-06	2022-07	2022-08	2022-09	2022-10
HIGH	1	1	1	1	1	5
MEDIUM	2	3	2	3	3	8
LOW	0	0	0	0	1	1
SHARED	0	1	1	1	1	1

Arctic EWS shows you a **history of unique issues** affecting the registered assets. It is a convenient way to track how the security posture changes over time. For Arctic EWS subscribers, history is based on timely matches against the registered assets. We built Arctic EWS to help you achieve a “green” report, and to fix discovered issues as soon as they are detected.

Report Description

The purpose of the Performance and Progression Report is to inform you about your publicly available network resources and detail observed threats related to them. The report goes back up to six months into the history, depending on how long you have been a customer of this service.

Discovered Issues

The numbers in the monthly assessment reflect all unique threats linked to your network assets. Each threat is described through a dedicated page in the report, which are grouped by the asset in question. Up to 200 pages with observations over the past month are included into this report. We describe each threat in a way that helps you understand what the threat is, why it is a problem and how to validate it.

Severity Ratings

The severity rating describes the urgency of the situation. A high severity observation needs to be triaged immediately. A medium severity observation can be dealt with through normal operations and a low severity observation is something you should keep an eye on. Threat type definitions are described in a separate section of this report.

Asset Discovery

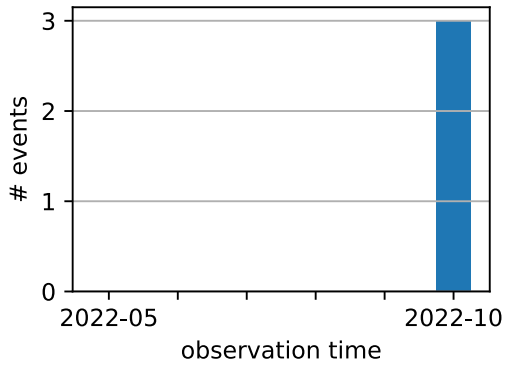
The asset discovery enumerates all the domain names under the maximum of five domains you have supplied us and in this report we list up to 10000 domain names related to each. In addition, we resolve the domain names to their respective IP addresses and name the network owners for those addresses.

Security Posture

The only way to be able to secure your organization is to know your network assets. This report details all the observed threats related to you, which are visible to the outside. With this information you will be able to secure your services and users in a more efficient way, monitor your performance and track your progression over time.

High Severity Observations

HIGH | 198.51.100.1



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
62

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC

Observation time in the history chart shows when this problem was first seen and how often. Much of the data is available for anyone who purchases it or finds it themselves. **You should receive this information before anyone has time to exploit the problem.**

BOTNET DRONE

WHAT IS THIS OBSERVATION?
Malware infected machines are often part of a botnet and reach out to a command and control server for operating instructions.

WHY IS THIS A PROBLEM?
The affected host has been infected by a piece of malware and is under the control of a third party malicious actor.

HOW CAN I VALIDATE THIS?
Triage the observation with the help of your ICT personnel.

source time	port	destination port	destination ip	protocol	malware family
2022-10-19 00:31:32Z	22077	443	72.21.81.200	tcp	cobaltstrike
2022-10-18 00:00:14Z	46333	443	72.21.81.200	tcp	cobaltstrike
2022-10-17 19:57:20Z	61247	443	72.21.81.200	tcp	cobaltstrike

Source time in this list of observations tells you when our data provider noticed this problem. Use these times to identify the affected system in your network. The table shows the last six observations, although there may have been more. Information from this table is included in the daily notifications you receive from Arctic EWS.

Port, destination port, destination ip and protocol provide you details necessary to pinpoint the system in your network, in case the ip address of the observation is for your firewall or a proxy server.

Malware family helps you in your triage, so that you know what actions to take to begin the incident response process for this issue.

HIGH | 198.51.100.14

IP address that was observed to have the problem described on this page.

Matching data tells you what asset linked this observation to you; in this example, it is a range of IP addresses that you control.

MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
1

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

The **network owner** is based on public information on whose network this asset is hosted. If the information is inaccurate, it is good to ensure that your public records are up to date.

VULNERABLE SERVICE

WHAT IS THIS OBSERVATION?
The OpenSSL library exposes a severe flaw, which can allow malicious unauthenticated third parties to obtain the server's private key.

VULNERABILITY
heartbleed

SERVICE
ssl/tls

ADDITIONAL INFORMATION
https://heartbleed.com/

The service description on this page provides high-level information on why this is a serious problem and how to validate the reported issue. Arctic EWS focuses on **actionable data on issues you can fix**.

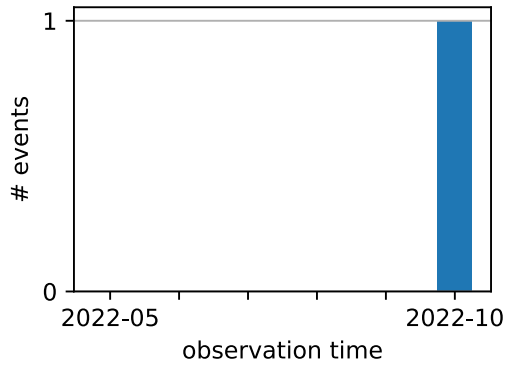
WHY IS THIS A PROBLEM?
The private key of the affected server used to protect SSL connections in the hands of the attacker can expose all the contents of the protected communication between a client and a server.

HOW CAN I VALIDATE THIS?
Check your OpenSSL version.

source time	port	protocol	transport protocol	description url
2022-10-26 03:36:20Z	80	ssl/tls	tcp	https://www.shodan.io/host/..

When additional information is available, Arctic EWS notifications provide links to the source material for context.

MEDIUM | 198.51.100.14



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
1

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC
AU

VULNERABLE SERVICE

WHAT IS THIS OBSERVATION?
OpenSSL implementations on client and server side suffer from a vulnerability, dubbed FREAK, that allows a downgrade of the secure communications to a weak cipher (due to past export controls exercised by the USA).

VULNERABILITY
CVE-2015-0204

SERVICE
ssl/tls

ADDITIONAL INFORMATION
Even if the vulnerability directly affects TLS/SSL clients, it may be used to gain access to the vulnerable server through a compromised client connection.

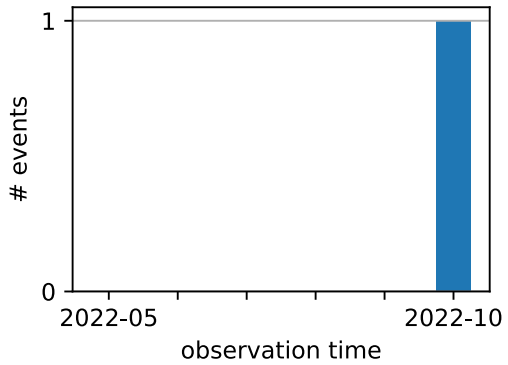
WHY IS THIS A PROBLEM?
The ability for a malicious third party to downgrade the communication to a weak cipher they can break, exposes the protected communication to further exploitation.

HOW CAN I VALIDATE THIS?
Verify the OpenSSL version of the affected system.

source time	port	protocol	transport protocol	description url
2022-10-26 03:36:20Z	80	ssl/tls	tcp	https://www.shodan.io/host/..

The observation pages are grouped by the IP address. When the same IP address has both high and medium severity observations, the medium severity incident can be found directly after the high severity observation in the report.

HIGH | 198.51.100.17



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
1

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC
AU

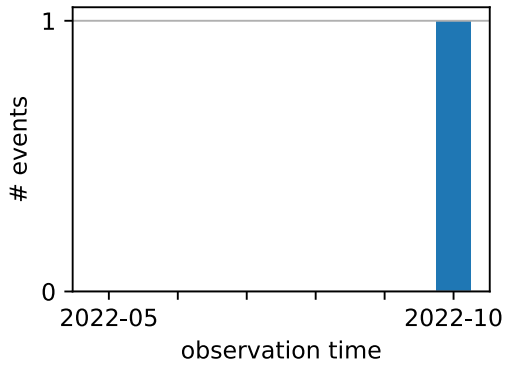
VULNERABLE SERVICE

WHAT IS THIS OBSERVATION?
Pulse Connect Secure SSL VPN exposes a severe vulnerability, which leads to remote code execution.
VULNERABILITY
CVE-2021-22893
SERVICE
pulse connect ssl vpn
ADDITIONAL INFORMATION
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/

WHY IS THIS A PROBLEM?
Exploitation of this vulnerability allows third parties to bypass the VPN and intercept all VPN tunnels.
HOW CAN I VALIDATE THIS?
Check which version of the software you are running.

description	vulnerability	service	additional information
This host is running a version of the Pulse Connect Secure gateway software, which is most likely vulnerable to remote code execution through the web interface.	CVE-2021-22893	pulse connect ssl vpn	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/

HIGH | 198.51.100.18



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
3

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC
AU

COMPROMISED SERVER

WHAT IS THIS OBSERVATION?
SolarWinds® Orion is a popular IT monitoring platform.

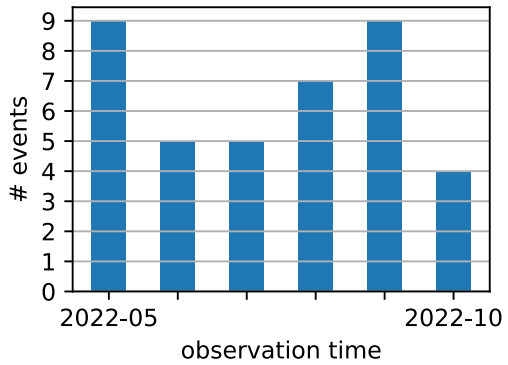
ADDITIONAL INFORMATION
https://cyber.dhs.gov/ed/21-01/

WHY IS THIS A PROBLEM?
The US CISA has publicly stated that the source code compromise and subsequent malicious access to these servers were the work of Russian Foreign Intelligence Service (SVR). In addition, exposing this monitoring system directly to the Internet is a bad idea.

HOW CAN I VALIDATE THIS?
Make sure that you have taken all the necessary actions recommended by the CISA emergency directive to validate that the threat actors have not persisted in your networks. In addition, make sure that your Solarwinds Orion server is not directly exposed to the Internet.

source time	port	protocol	transport protocol	description url
2023-07-25 05:24:48Z	443		tcp	https://www.shodan.io/host/..

HIGH | 198.51.100.2



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
9

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC
AU

VULNERABLE SERVICE

WHAT IS THIS OBSERVATION?
Microsoft IIS 6.0 WebDav service has severe flaw, which allows malicious third parties to execute arbitrary commands on the server within the context of the running application.

VULNERABILITY
CVE-2017-7269

SERVICE
iis webdav

ADDITIONAL INFORMATION
https://docs.microsoft.com/en-us/security-updates/securityadvisories/2017/4025685

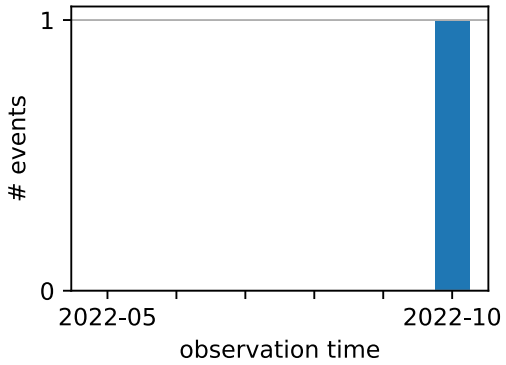
WHY IS THIS A PROBLEM?
Microsoft discontinued support for IIS 6.0 in 2015. In practice this means that there is no fix for this flaw other than redeploying the service on a newer supported platform.

HOW CAN I VALIDATE THIS?
Double check whether you are running IIS 6.0 on this server.

source time	port	protocol	transport protocol	description url
2022-10-31 22:25:10Z	443	http	tcp	https://www.shodan.io/host/..
2022-10-27 18:45:57Z	443	http	tcp	https://www.shodan.io/host/..
2022-10-16 19:34:06Z	443	http	tcp	https://www.shodan.io/host/..
2022-10-05 04:11:46Z	443	https	tcp	https://www.shodan.io/host/..

Medium Severity Observations

MEDIUM | 198.51.100.11



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
4

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC
AU

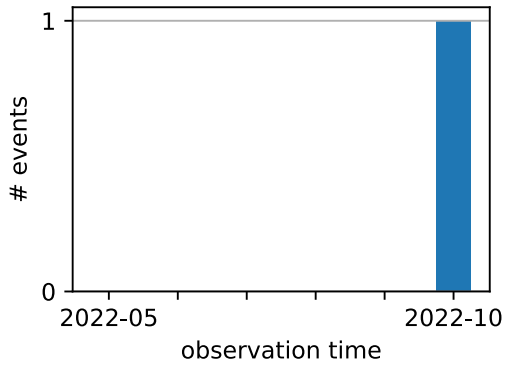
VULNERABLE SERVICE

WHAT IS THIS OBSERVATION?
Remote Desktop Protocol, is a handy way to access a machines desktop over the network.
VULNERABILITY
exposed rdp
SERVICE
remote desktop
ADDITIONAL INFORMATION
https://www.cloudflare.com/learning/access-management/rdp-security-risks/

WHY IS THIS A PROBLEM?
Exposing RDP to the Internet is not a good idea, since it is being actively used as an entry vector by ransomware operators for example.
HOW CAN I VALIDATE THIS?
Check that RDP is not exposed to the Internet on port TCP/3389.

source time	port	protocol	transport protocol	description url
2022-10-26 03:37:04Z	3389	rdp	tcp	https://www.shodan.io/host/..

MEDIUM | 198.51.100.12



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
7

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC
AU

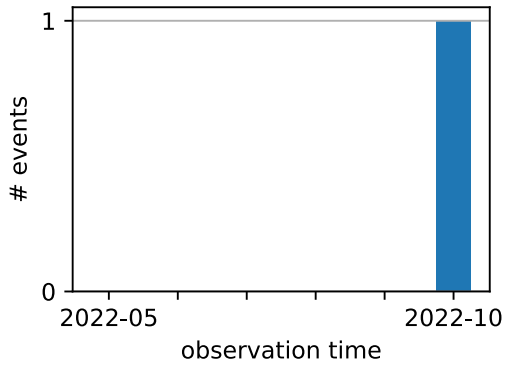
VULNERABLE SERVICE

WHAT IS THIS OBSERVATION?
The Kubernetes API is a management interface to a Kubernetes cluster.
VULNERABILITY
exposed kubernetes api
SERVICE
kubernetes api
ADDITIONAL INFORMATION
https://kubernetes.io/docs/concepts/security/controlling-access/

WHY IS THIS A PROBLEM?
Exposing a management interface to the whole Internet is a bad idea, since a breach of the interface will compromise the security of the whole cluster.
HOW CAN I VALIDATE THIS?
Validate that the API is not exposed to the whole Internet.

source time	port	protocol	description url
2022-10-26 03:35:30Z	443	http	https://www.shodan.io/host/..

MEDIUM | 198.51.100.13



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
3

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC
AU

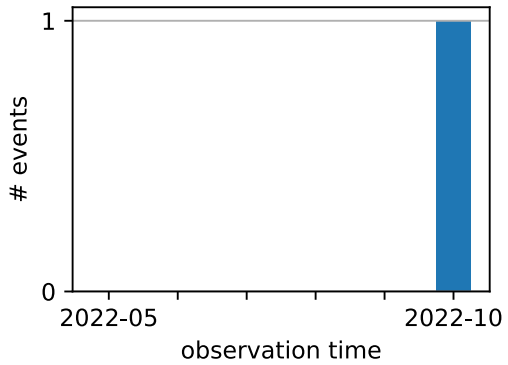
VULNERABLE SERVICE

WHAT IS THIS OBSERVATION?
Server Message Block, SMB, is a common way to create networked file shares for a local network environment.
VULNERABILITY
exposed smb
SERVICE
smb service

WHY IS THIS A PROBLEM?
SMB was never intended to be used over the Internet and exposing it can jeopardize the information stored on your file server. SMB has suffered from multiple security issues and has even some design flaws related to authentication and authorization.
HOW CAN I VALIDATE THIS?
Verify that your SMB share is not exposed to the Internet on TCP/445.

source time	port	protocol	transport protocol	description url
2022-10-26 03:35:54Z	445	smb	tcp	https://www.shodan.io/host/..

MEDIUM | 198.51.100.15



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
3

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC
AU

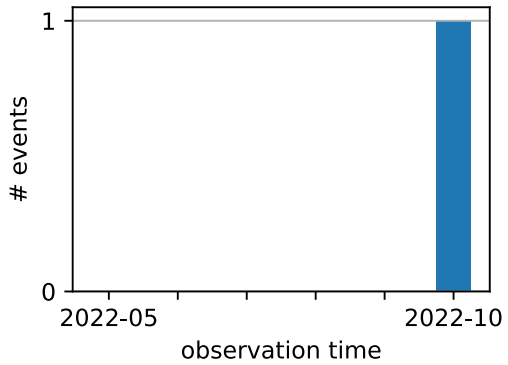
VULNERABLE SERVICE

WHAT IS THIS OBSERVATION?
FortiGate devices offer a next generation firewall and VPN service in the same solution.
VULNERABILITY
exposed fortigate management interface
SERVICE
fortigate management
ADDITIONAL INFORMATION
https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/303168/fortigate-open-ports

WHY IS THIS A PROBLEM?
Exposing a management interface to the Internet can jeopardize the security of all the systems which the firewall is tasked to protect.
HOW CAN I VALIDATE THIS?
Verify that the management interface is not exposed to the Internet on TCP/541.

source time	port	protocol	description url
2022-10-26 03:33:34Z	541		https://www.shodan.io/host/..

MEDIUM | 198.51.100.16



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
2

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC
AU

VULNERABLE SERVICE

WHAT IS THIS OBSERVATION?
Hosts subject to these observations have been observed to expose a vulnerability to the Internet which may be abused by a third party.

VULNERABILITY
CVE-2022-22536

SERVICE
sap java

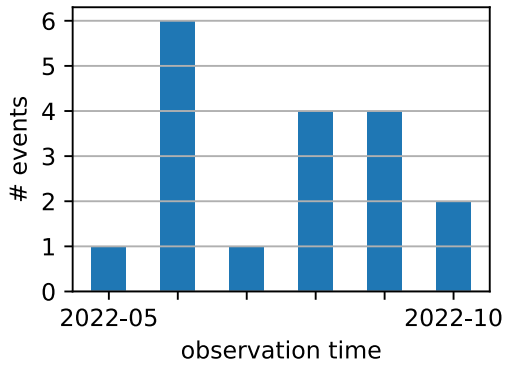
ADDITIONAL INFORMATION
https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+February+2022

WHY IS THIS A PROBLEM?
Depending on the observed issue, the vulnerability or weakness may lead to unauthorized use of the affected service by a malicious third party.

HOW CAN I VALIDATE THIS?
Triage the observation with the help of your ICT personnel.

source time	port	protocol	transport protocol
2022-10-26 03:44:03Z	443	http	tcp

MEDIUM | 198.51.100.5



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
2

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC
AU

VULNERABLE SERVICE

WHAT IS THIS OBSERVATION?
MySQL is a database engine, which can be accessed over the network or through UNIX sockets.

VULNERABILITY
exposed mysql

SERVICE
mysql database

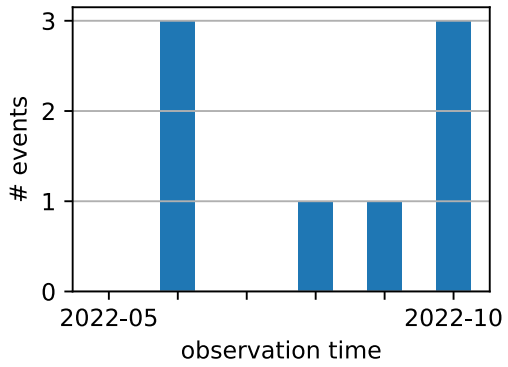
ADDITIONAL INFORMATION
By default, database services should not be directly exposed to the Internet.

WHY IS THIS A PROBLEM?
Exposing a SQL backend service directly to the Internet is a bad idea, since this has lead into serious data breaches without any defense in depth.

HOW CAN I VALIDATE THIS?
Verify that the MySQL service is not exposed to the Internet on TCP/3306.

source time	port	protocol	transport protocol	description url
2022-10-31 21:15:55Z	3306	mysql	tcp	https://www.shodan.io/host/..
2022-10-30 12:35:47Z	3306	mysql	tcp	https://www.shodan.io/host/..

MEDIUM | 93.184.216.34



MATCHING DATA
example.com

DOMAIN NAME COUNT
9999

NETWORK NAME
EDGECAST-NETBLK-03

NETWORK OWNER
EdgeCast Networks, Inc

NETWORK RANGE
93.184.216.0/24

CC
US

ASN
15133

AS NAME
EDGECAST, US

BGP PREFIX
93.184.216.0/24

VULNERABLE SERVICE

WHAT IS THIS OBSERVATION?
X.509 is an essential part in verifying the parties doing the communication for TLS protected implementations. Expired X.509 certificates put these protected communications at risk.

VULNERABILITY
expired x509 certificate

SERVICE
ssl/tls

WHY IS THIS A PROBLEM?
The root cause for one of the biggest data breaches related to online payment systems was due to the fact that the security monitoring systems for the affected organization had expired X.509 certificates.

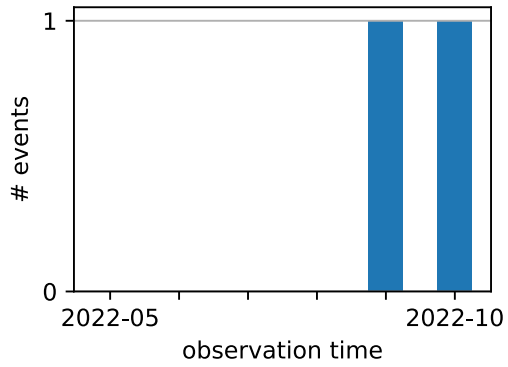
HOW CAN I VALIDATE THIS?
Verify that the certificate tied to your protected communication has not expired.

source time	port	product	x509 subject cn	x509 not after
2022-10-30 08:56:03Z	443	Apache httpd	www.example.com	2019-08-13 12:00:00Z
2022-10-24 23:13:31Z	443	Apache httpd	www.example.com	2019-08-13 12:00:00Z
2022-10-15 21:14:45Z	443	Apache httpd	www.example.com	2019-08-13 12:00:00Z

Low Severity Observations

- 198.51.100.6 21

LOW | 198.51.100.6



MATCHING DATA
198.51.100.0/24

DOMAIN NAME COUNT
6

NETWORK NAME
TEST-NET-2

NETWORK OWNER
APNIC Research and Development

NETWORK RANGE
198.51.100.0/24

CC
AU

OPEN SERVICE

WHAT IS THIS OBSERVATION?
Rsync is an efficient data transfer protocol, especially for mirroring large data sets between two hosts.

SERVICE
rsync daemon

ADDITIONAL INFORMATION
protocol version 31

WHY IS THIS A PROBLEM?
Exposing the rsync daemon to the Internet can be useful for public data repositories, but secure/private use of the protocol must rely on SSH and no daemon is needed.

HOW CAN I VALIDATE THIS?
Make sure that rsync daemon is not unintentionally exposed to the Internet on TCP/873.

source time	port	protocol	transport protocol	description url
2022-10-11 16:36:29Z	873	rsync	tcp	https://www.shodan.io/host/..

Leaked Credentials

The following table contains a summary of leaked credentials discovered on the dark web associated with the domain names you have supplied us for monitoring. The actual details have been shared with you either through email notifications or through Leaked Credentials Data API.

The table lists the following fields: the domain name indicates the monitored domain, the source time denotes the year when the credentials were leaked, the email addresses shows the number of unique addresses leaked, the passwords counts unique passwords in the data and the sources denotes the number of unique data dumps from which the leaked credentials have been extracted.

domain name	source time	email addresses	passwords	sources
example.com	2022	6	5	0

Observations on Shared Resources

The observations below are related to the domain names in your customer configuration. Based on our analysis, IP addresses for these domains are likely shared between multiple organizations, making them shared resources. A vendor-hosted SaaS service that uses your domain is a typical example.

Below each finding, we list the domain names associated with the IP address of the observation if they do not match any of the domain names in your current configuration. If you see domains that belong to you in this list, please add them to your configuration.

matching data	domain name count	severity	type	description	last seen
93.184.216.34 ⓘ	9999	medium	open service	This host is most likely exposing a BGP interface to the Internet. Current best practices recommend limiting connections to the BGP port to ips of known BGP neighbours.	2022-10-31
nonmatching domains: service-provide.example					

Service providers may also suffer from vulnerabilities that can place your organization and your data at risk. We classify systems hosting multiple domains (9999 in this example) as a shared resource.

Your risk with these assets is more likely to be reputational, since they can affect your security ratings. You may also be at real risk if the underlying host system becomes compromised.

Network Assets

The table below details the IP addresses and networks you have supplied us. For each asset we list the network owner and country code, which are based on whois information.

network owner	cc	ip addresses
APNIC Research and Development	AU	198.51.100.0/24

Network information about the assets are provided to Arctic EWS by the subscriber.

We only report about problems on assets that you are interested in, and problems you are able to fix.

You can list all of your assets without limitations, Arctic EWS subscription is not based on asset count.

Static Domain Names

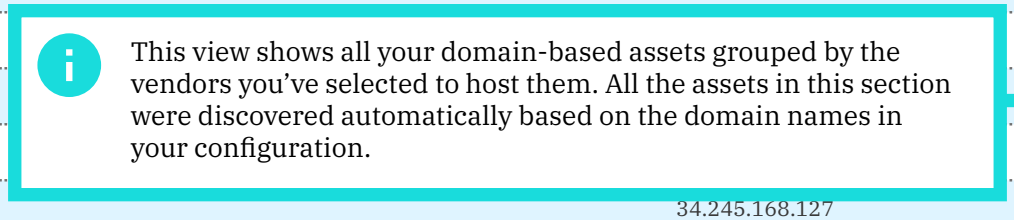
The table below details the domain names you have supplied us to be used as part of the Arctic Early Warning Service. If a domain name resolves to one or more IPs, we list them in the same table, as well as the network owners for those IPs.

domain name	ip				network owner
example.com	2606:2800:220:1:248:1893:25c8:1946				
example.com	93.184.216.34				EdgeCast Networks, Inc
arcticsecurity.com	185.199.108.153	185.199.109.153	185.199.110.153	185.199.111.153	Git Hub

Enumerated Domain Names

The table below enumerates all the domain names, which associate to the domains you have supplied us. The domain names are grouped by network owners, which in turn are determined through the resolved IPs.

domain name		ip	network owner
hub-pidele.arcticsecurity.com	pidele.arcticsecurity.com		
c5demo.arcticsecurity.com		35.183.44.113	Amazon Data Services
cert-be.arcticsecurity.com		52.17.139.188	Amazon Data Services
api.ews.arcticsecurity.com		52.30.31.14	Amazon Data Services
bs.ews.arcticsecurity.com		34.255.131.85	Amazon Data Services
csf.ews.arcticsecurity.com		34.241.145.214	Amazon Data Services
csv.ews.arcticsecurity.com		52.17.41.116	Amazon Data Services
reporting.ews.arcticsecurity.com		52.31.31.23	Amazon Data Services
shadowserver.ews.arcticsecurity.com			Amazon Data Services
ssapi.ews.arcticsecurity.com			Amazon Data Services
feedscollector1.arcticsecurity.com			Amazon Data Services
feedscollector2.arcticsecurity.com		34.245.168.127	Amazon Data Services
feedscollector3.arcticsecurity.com		3.249.95.72	Amazon Data Services
feedshub.arcticsecurity.com		52.17.89.62	Amazon Data Services
feedshub-sg.arcticsecurity.com		18.138.45.2	Amazon Data Services
furoko.arcticsecurity.com		13.246.13.223	Amazon Data Services
hub-qebula.arcticsecurity.com	qebula.arcticsecurity.com	34.244.119.60	Amazon Data Services
ifobir.arcticsecurity.com		3.253.20.143	Amazon Data Services



domain name		ip	network owner
noc.arcticsecurity.com		13.51.145.122	Amazon Data Services
pwc.arcticsecurity.com		3.249.102.65	Amazon Data Services
ssh-eu.arcticsecurity.com		13.49.79.170	Amazon Data Services
stg-ews.arcticsecurity.com		34.254.66.180	Amazon Data Services
history.stg-ews.arcticsecurity.com		34.240.55.69	Amazon Data Services
yarala.arcticsecurity.com		16.16.66.36	Amazon Data Services
honeypot.arcticsecurity.com		79.125.127.47	Amazon EU
chat.arcticsecurity.com		54.155.138.166	Amazon Technologies Inc
demonode-sg.arcticsecurity.com		18.140.2.211	Amazon Technologies Inc
history.ews.arcticsecurity.com		54.170.76.222	Amazon Technologies Inc
ssh-jp.arcticsecurity.com		54.178.90.167	Amazon Technologies Inc
ssh-sg.arcticsecurity.com		54.169.92.102	Amazon Technologies Inc
hub-partner.stg-ews.arcticsecurity.com	partner.stg-ews.arcticsecurity.com	54.170.79.87	Amazon Technologies Inc
reporting.stg-ews.arcticsecurity.com		54.74.97.43	Amazon Technologies Inc
aws-node-register.arcticsecurity.com		108.157.229.108 108.157.229.126 108.157.229.4 108.157.229.52 2600:9000:2395:4800:1d:6f01:380:93a1 2600:9000:2395:4e00:1d:6f01:380:93a1 2600:9000:2395:8000:1d:6f01:380:93a1 2600:9000:2395:d000:1d:6f01:380:93a1 2600:9000:2395:d400:1d:6f01:380:93a1 2600:9000:2395:de00:1d:6f01:380:93a1 2600:9000:2395:ee00:1d:6f01:380:93a1 2600:9000:2395:f200:1d:6f01:380:93a1	Amazon.com, Inc
ews.arcticsecurity.com		54.220.238.13	Amazon.com, Inc

domain name		ip	network owner
feedshub.ews.arcticsecurity.com		63.35.179.139	Amazon.com, Inc
arcs1.arcticsecurity.com dev-ews.arcticsecurity.com csf.stg-ews.arcticsecurity.com	smtp.arcs1.arcticsecurity.com jenkins.arcticsecurity.com	178.213.233.200	F-Solutions Oy
arcs2.arcticsecurity.com		178.213.233.201	F-Solutions Oy
arcs5.arcticsecurity.com	research-feedshub.arcticsecurity.com	178.213.233.202	F-Solutions Oy
arcs1.arcticsecurity.com dev-ews.arcticsecurity.com csf.stg-ews.arcticsecurity.com	smtp.arcs1.arcticsecurity.com jenkins.arcticsecurity.com	2a00:4cc1:6:1007::1001	F-Solutions Oy North
arcs5.arcticsecurity.com	research-feedshub.arcticsecurity.com	2a00:4cc1:6:1007::1003	F-Solutions Oy North
arcs3.arcticsecurity.com		37.35.86.69	Fiber Co-Operative Network
backup.arcticsecurity.com		37.35.86.70	Fiber Co-Operative Network
www.arcticsecurity.com		199.60.103.2 199.60.103.254 2606:2c40::c73c:6702 2606:2c40::c73c:67fe	HubSpot LLC

domain name	ip	network owner
www.example.com	2606:2800:220:1:248:1893:25c8:1946	
www.example.com	93.184.216.34	EdgeCast Networks, Inc

Further Information

Threat Type Definitions

We map all the incoming observations with our functional types based on original details present in the source data.

Type	Description	Impact
artifact	Artifacts refer to host-based indicators, such as checksums, file paths.	These indicators do not directly reference a compromise, rather can be used for monitoring and detection.
attribution	Indicators which can be attributed to malicious activity without a specific functional category such as a command and control server.	These indicators attribute infrastructure to potential actors, but cannot be directly used for victim notification, since the nature of the compromise is often unspecified
backdoor	Backdoor indicators refer to hosts which have been compromised and/or backdoored by a third party.	Threat actors may use this functionality to gain remote access to the machine or service.
blacklist	Some sources provide blacklists which clearly refer to abusive behavior (such as spamming) but fail to denote the exact reason why a given identity has been blacklisted. The justification may be anecdotal or missing entirely. This type should only be used if the typing fits the definition of a blacklist, but an event specific denomination is not possible for one reason or another.	Blacklisted services will have difficulty to operate normally, as their service specific communication will be blocked by third parties.
botnet drone	The most numerous type of abuse, as it refers to compromised computers calling out to a command and control mechanism.	These hosts are most likely infected by a piece of malware and controlled by the threat actors.
brute-force	A machine which has been observed to perform brute-force attacks over a given application protocol, e.g. ssh	These hosts are most likely infected by malware or compromised and are trying to break into other computers or services.
c&c	A command and control server in charge of a given number of botnet drones.	This computer or service is controlling a botnet and functioning as part of the threat actor infrastructure.
compromised account	A user account which has been compromised by a third party.	These compromised user accounts may lead to further unauthorized use through password re-use even if the compromised service is not part of the victim infrastructure.
	This server or service has been compromised by a third party.	

Type	Description	Impact
compromised server		These hosts or services are under the threat actor control to do their bidding.
ddos infrastructure	This type refers to various parts of DDoS botnet infrastructure.	These hosts or services have most likely facilitated DDoS attacks even if they have not been necessarily compromised. They may for example offer a UDP-based vulnerable service, which has been spoofed to facilitate a reflected attack against a third party. This in turn may consume the upstream bandwidth of the host during an attack.
ddos target	This type refers to the intended target of a DDoS attack: the intended domain name or IP address.	This host or service will most likely be unavailable because of the DDoS attack.
defacement	This type refers to hacktivism, which on a technical level is an indicator of a compromised service.	This host is compromised by a third party and very often is used for other criminal activities as well.
dropzone	This type refers to a resource which is used to store stolen user data.	PII is often stored unlawfully on these hosts or services.
exploitation	This type refers to attempted or successful exploitation of a vulnerable service.	A successful exploitation of a vulnerable service will lead to unauthorized use of this host or service.
exploit url	An exploit or an exploit kit is often served through a malicious URL.	These URLs are used by the threat actors to spread malware. These hosts or services are often compromised to facilitate this activity.
ids alert	Alerts from a heuristic sensor network. This is a generic classification, as often the taxonomy of these types of events lack consistency.	These indicators denote potential malicious activity either in the network traffic or system logs.
malware configuration	This is a resource which updates botnet drones with a new configurations.	These hosts or services function as part of threat actor infrastructure and are often compromised by threat actors.
malware url	A URL is the most common resource with reference to malware binary distribution.	These hosts are serving pieces of malware to infect new machines and are usually compromised by the threat actors.
open service	This type refers to network services, which are publicly exposed to the Internet. This may be intentional or the result of a misconfiguration.	Even if scanning for this service has not identified a specific vulnerability, unintentionally exposed network services increase the attack surface and may lead to compromise.

Type	Description	Impact
phishing	This type most often refers to a URL which is trying to defraud the users of their credentials.	These URLs are served to potential victims to try to steal their credentials to a third party service. These hosts are often compromised by threat actors.
ransomware	This type refers to a specific type of compromised machine, where the computer has been hijacked for ransom by the criminals.	The disk resources of these hosts are encrypted by the criminals for ransom or sabotage. This may lead to the encryption of disk resources for an entire organization.
scanner	This type refers to port or vulnerability scanning attempts in general.	These hosts are scanning for vulnerable services to enable threat actors to compromise them. The host doing the scanning are often compromised or infected as well.
spam infrastructure	This type refers to resources which make up a spammer's infrastructure, be it a harvester, dictionary attacker, URL, spam etc.	These hosts will most likely get blacklisted because they are participating in spamming activities.
test	Used for testing purposes.	These events can be used to test a victim notification pipeline for example, without impacting the functionality of the service.
vulnerable service	This type refers to poorly configured or vulnerable network service, which may be abused by a third party. For example, these services relate to open proxies, open DNS resolvers, network time servers (NTP), character generation services (CharGen) or simple network management services (SNMP). In addition, to specify the network service and its potential abuse, one should also use the protocol, port and description attributes.	These services make it easy for the threat actors to perform their deeds without having to necessarily compromise a large number of hosts on the Internet.

Malware Families Tracked by Arctic EWS

The table below enumerates all the malware families reported by our sources for suspected compromise.

Adwind	AgentTesla	ArkeiStealer	AsyncRAT	BitRAT
BlackGuard	BumbleBee	CobaltStrike	DCRat	DanaBot
DarkWatchman	Gozi	IceXLoader	Malware	Matanbuchus
NanoCore	Neurevt	OrcusRAT	Ousaban	PhoenixRAT
QuasarRAT	RM3	RaccoonStealer	RedLineStealer	ServHelper
Smoke Loader	Vjw0rm	abstealer	acruxminer	adware_multiplug
adware_opencandy	aldibot	amadey	android_rottensys	andromeda
avalanchebotnet-andromeda	avalanchebotnet-bolek	avalanchebotnet-citadel	avalanchebotnet-corebot	avalanchebotnet-dofoil
avalanchebotnet-gozi2	avalanchebotnet-goznym	avalanchebotnet-kins	avalanchebotnet-marcher	avalanchebotnet-matsnu
avalanchebotnet-nymaim	avalanchebotnet-pandabanker	avalanchebotnet-ranbyus	avalanchebotnet-rovnix	avalanchebotnet-smartapp
avalanchebotnet-teslacrypt	avalanchebotnet-tinba	avalanchebotnet-trusteer	avalanchebotnet-urlzone	avalanchebotnet-vawtrak
avalanchebotnet-xswkit	azorult	backdoor_solarbot	banload	bazarloader
betabot	blackenergy	bluebot	bolek	bumblebee
cenjonsla	citadel	citeary	cobaltstrike	conficker
corebot	coresys	crowti	darkcomet	ddosbot_meris
ddoser	diamondfox	dirtjumper	dofoil	domaiq adware
dorkbot	dridex	emotet	enfal	ezbro
feodo	gamarue	godzilla	gozi2	goznym

graybird	gumblar	isrstealer	jadtre	jedobot
kasidet	katrina	keybase	kins	kpot
kratos	kronos	locky	lokibot	madness
marcher	matsnu	meris	minerpanel	mirai
mobile_hiddenads	mobile_pareto	multiplug adware	nanocore	neconyd
neverquest	nymaim	opencandy adware	optima	palevo
pandabanker	pandora	pareto	pincher	ponyloader
poseidon	poseidon-findstr	predatorthethief	proxyback	pua
pushdo/cutwail	pykspa	qakbot	quant	raccoonstealer
ramnit	ranbyus	redline	rovnix	sality
sdbot	simda	smartapp	smokeloader	socks
solar	solarbot	stabuniq	stealrat	stration worm
suprememiner	swisyn	teslacrypt	tinba	trickbot
trojan_upatre	trusteer	tsunami	umbra	unnamed_botnet
upatre	urlzone	vawtrak	vertexnet	viking
virus_ramnit	wapomi	wonton	xorddos	xswkit
zeus	zezin			

Vulnerabilities Tracked by Arctic EWS

The table below enumerates all the vulnerabilities which are reported by our sources for vulnerable services.

CVE-2013-1899	CVE-2014-9222	CVE-2015-0204	CVE-2015-1635	CVE-2015-2080
CVE-2015-4000	CVE-2017-7269	CVE-2019-0708	CVE-2019-10149	CVE-2019-11510
CVE-2019-1653	CVE-2019-19781	CVE-2020-0688	CVE-2020-0796	CVE-2020-11651
CVE-2020-12695	CVE-2020-1938	CVE-2020-2021	CVE-2020-5902	CVE-2021-22893
CVE-2021-26084	CVE-2021-3060	CVE-2021-31206	CVE-2021-3449	CVE-2021-40539
CVE-2021-41773	CVE-2021-42013	CVE-2022-22536	CVE-2022-26134	expired x509 certificate
exposed 6to4 relay	exposed SAP router	exposed ad ldap	exposed adb	exposed afp
exposed amt	exposed apache airflow	exposed ard	exposed bacnet	exposed cassandra db
exposed cisco configuration interface	exposed cisco smart install interface	exposed cisco web management	exposed citrix nsip	exposed citrix virtual application server
exposed coap	exposed couchdb	exposed cpanel	exposed db2	exposed docker daemon
exposed elasticsearch	exposed f5 management interface	exposed flexnet license manager	exposed fortigate management interface	exposed fortinet management interface
exposed grandstream management interface	exposed gtp	exposed hikvision web camera	exposed imap	exposed influxdb
exposed ipmi	exposed ipp	exposed jenkins dashboard	exposed kubernetes api	exposed mdns
exposed memcache daemon	exposed memcached	exposed modbus	exposed mongodb	exposed moxa nport
exposed mqtt	exposed ms rpc	exposed ms-sql	exposed ms-sql browser service	exposed mssql browser interface

exposed mysql	exposed niagara fox	exposed omron plc	exposed oracle xml db	exposed pbx console
exposed polycom configuration interface	exposed pop3	exposed postgres	exposed rabbit microcontroller	exposed rdp
exposed redis	exposed riak db	exposed router management	exposed rtu web interface	exposed servlet service
exposed siemens plc	exposed smb	exposed snmp	exposed sophos web portal	exposed ssdp
exposed supermicro ipmi	exposed telnet	exposed tftp	exposed vmware console	exposed vnc
exposed weblogic	exposed wind farm portal	exposed winrm	exposed zyxel web management	heartbleed
misconfiguration	multiple cves	obsolete service	open proxy	recursive dns resolver
ssh1	sslv2	vulnerable openssl		

Open Services Tracked by Arctic EWS

The table below enumerates all the services exposed to the Internet which we track to help you keep on top of services which may be unintentionally exposed to the Internet or have a mottled history with information security.

adb1	adb2	adb3	bgp	citrix gateway
citrix mgmt	exposed rsync	f5 tmos	fortigate 100d	fortios
ms exchange servers	open rsync	open vpn service	panasonic devices	remote screenshots
sonicwall ssl vpn	zscaler infrastructure			