STORM WATCH

CYBERSECURITY NEWS

Dateline: 2024-07-29

LIKE

SUBSCRIBE

Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (https://www.greynoise.io), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

https://StormWatch.ing

LEAVE A COMMENT

SHARE


LIVE
BREAKING
NEWS

DigiCert Revocation Incident (CNAME-Based Domain Validation)

July 29, 2024

https://www.digicert.com/support/certificate-revocation-incident

DigiCert will be revoking certificates that did not have proper Domain Control Verification (DCV). Before issuing a certificate to a customer, DigiCert validates the customer's control or ownership over the domain name for which they are requesting a certificate using one of several methods approved by the CA/Browser Forum (CABF). One of these methods relies on the customer adding a DNS CNAME record which includes a random value provided to them by DigiCert. DigiCert then does a DNS lookup for the domain and verifies the same random value, thereby proving domain control by the customer.

There are multiple valid ways to add a DNS CNAME record with the random value provided for this purpose. One of them requires the random value to be prefixed with an underscore character. The underscore prefix ensures that the random value cannot collide with an actual domain name that uses the same random value. While the odds of that happening are practically negligible, the validation is still deemed as non-compliant if it does not include the underscore prefix.

Recently, we learned that we did not include the underscore prefix with the random value used in some CNAME-based validation cases. This impacted approximately 0.4% of the applicable domain validations we have in effect. Under strict CABF rules, certificates with an issue in their domain validation must be revoked within 24 hours, without exception

STORM WATCH

CYBERSECURITY NEWS

CYBERSIDE CHAT

```
net group “ESX Admins” /domain /add

net group “ESX Admins” username /domain /add
```

CVE-2024-37085

```
net group “ESX Admins” /domain /add

net group “ESX Admins” username /domain /add
```

Full administrative access on the ESXi hypervisor. O_O

https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

VMware ESXi hypervisors joined to an Active Directory domain consider any member of a domain group named “ESX Admins” to have **full administrative access by default**.

This group is not a built-in group in Active Directory and does not exist by default.

ESXi hypervisors do not validate that such a group exists when the server is joined to a domain and still treats any members of a group with this name with full administrative access, even if the group did not originally exist.

Additionally, the membership in the group is determined by name and not by security identifier (SID).

- Validate the group “ESX Admins” exists in the domain and is hardened.
- Manually deny access by this group by changing settings in the ESXi hypervisor itself. If full admin access for the Active Directory ESX admins group is not desired, you can disable this behavior using the advanced host setting: ‘`Config.HostAgent.plugins.hostsvc.esxAdminsGroupAutoAdd`’.
- Change the admin group to a different group in the ESXi hypervisor.
- Add custom detections in XDR/SIEM for the new group name.
- Configure sending ESXi logs to a SIEM system and monitor suspicious full administrative access.

STORM WATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT

JOINT
CYBERSECURITY ADVISORY

TLP:CLEAR

Product ID: AA24-207A

July 25, 2024

Co-Authored by:

National Cyber Security Centre
a part of GCHQ

North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs

Summary

The U.S. Federal Bureau of Investigation (FBI) and the following authoring partners are releasing this Cybersecurity Advisory to highlight cyber espionage activity associated with the Democratic People's Republic of Korea (DPRK)'s Reconnaissance General Bureau (RGB) 3rd Bureau based in Pyongyang and Sinuiju:

- U.S. Cyber National Mission Force (CNMF)
- U.S. Cybersecurity and Infrastructure Security Agency (CISA)
- U.S. Department of Defense Cyber Crime Center (DC3)
- U.S. National Security Agency (NSA)
- Republic of Korea's National Intelligence Service (NIS)
- Republic of Korea's National Police Agency (NPA)
- United Kingdom's National Cyber Security Centre (NCSC)

The RGB 3rd Bureau includes a DPRK (aka North Korean) state-sponsored cyber group known publicly as Andariel, Onyx Sleet (formerly PLUTONIUM), DarkSeoul, Silent Chollima, and Stonefly/Clasiopa. The group

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Andariel (also called Onyx Sleet, DarkSeoul, Silent Chollima, and Stonefly/Clasiop

Mainly targets defense, aerospace, nuclear, engineering, medical and energy entities to obtain sensitive technical information and intellectual property to advance North Korea's military and nuclear programs.

Primarily targeting the U.S. and South Korea, the group also poses a threat to entities in Japan and India.

Exploit vulnerabilities in public-facing web servers, particularly using known vulnerabilities.

CVE-2017-4946: VMware V4H and V4PA
🏷️ CVE-2019-0708: Microsoft Remote Desktop Services
CVE-2019-15637: Tableau
🏷️ CVE-2019-7609: Kibana
🏷️ CVE-2021-20028: SonicWall Secure Remote Access (SRA)
🏷️ CVE-2021-20038: SMA100 Apache httpd server (SonicWall)
CVE-2021-3018: IPeakCMS 3.5
CVE-2021-36955: Windows log file vulnerability
CVE-2021-40684: Talend ESB Runtime
🏷️ CVE-2021-41773: Apache HTTP Server 2.4.49
CEV-2021-43207: Windows log file vulnerability
CVE-2021-43226: Windows log file vulnerability
CVE-2021-44142: Samba vfs_fruit module
🏷️ CVE-2021-44228: Apache Log4j
CVE-2021-45837: TerraMaster NAS
CVE-2022-21882: Win32k Elevation of Privilege
CVE-2022-22005: Microsoft SharePoint Server
🏷️ CVE-2022-22947: Spring Cloud Gateway
🏷️ CVE-2022-22965: Spring4Shell
CVE-2022-24663: PHP Everywhere
CVE-2022-24664: PHP Everywhere
CVE-2022-24665: PHP Everywhere
CVE-2022-24785: Moment.js
🏷️ CVE-2022-24990: TerraMaster NAS
CVE-2022-25064: TP-LINK
🏷️ CVE-2022-27925: Zimbra Collaboration Suite
CVE-2022-30190: Microsoft Windows Support Diagnostic Tool
CVE-2022-41352: Zimbra Collaboration Suite
🏷️ CVE-2022-47966: ManageEngine
🏷️ CVE-2023-0669: GoAnywhere MFT
CVE-2023-21932: Oracle Hospitality Opera 5
CVE-2023-25690: Apache HTTP Server
🏷️ CVE-2023-27997: FortiGate SSL VPN
CVE-2023-2868: Barracuda Email Security Gateway
CVE-2023-28771: Zyxell firmware
CVE-2023-3079: Google Chromium V8 Type Confusion
🏷️ CVE-2023-32315: Openfire
CVE-2023-32784: KeePass
CVE-2023-33010: Zyxell firmware
🏷️ CVE-2023-33246: RocketMQ
🏷️ CVE-2023-34362: MOVEIt
🏷️ CVE-2023-35078: Ivanti Endpoint Manager Mobile (EPMM)
🏷️ CVE-2023-3519: Citrix NetScaler
🏷️ CVE-2023-42793: TeamCity

They fund their espionage activity through ransomware operations against U.S. healthcare entities, and in some instances, the authoring agencies have observed the actors launching ransomware attacks and conducting cyber espionage operations on the same day and/or leveraging ransomware and cyber espionage against the same entity.

STORM WATCH

CYBERSECURITY NEWS

SHAMELESS SELF-PROMOTION

Tales from a Top Threat Buster

Attend our upcoming Black Hat USA speaking session, where the brilliant and fearless Dr. Venkman—oops, we mean, our esteemed Principal Security Researcher Emily Austin – explores the mind blowing magic of TLS certificates and how they quietly zap man-in-the-middle attacks.

When: Thursday, Aug. 8
Time: 10:20 a.m.
Location: Business Hall Theater D

Add to Calendar

Discover the Hidden Vulnerability Intelligence within CISA's KEV Catalog

Ground Floor, 14:30 Wednesday

Dive into the dynamic world of cybersecurity intelligence, focusing on the Known Exploited Vulnerabilities (KEV) catalog, initially crafted by the Cybersecurity and Infrastructure Security Agency (CISA) for government use but now a cornerstone across industries. Join me as I unravel the insights hidden within this treasure trove of exploit intelligence, offering a fresh perspective on prioritizing vulnerabilities in today's ever-evolving threat landscape.

Glenn Thorpe

Defensive Counting: How to quantify ICS exposure on the Internet when the data is out to get you

Ground Truth, 15:00 Tuesday

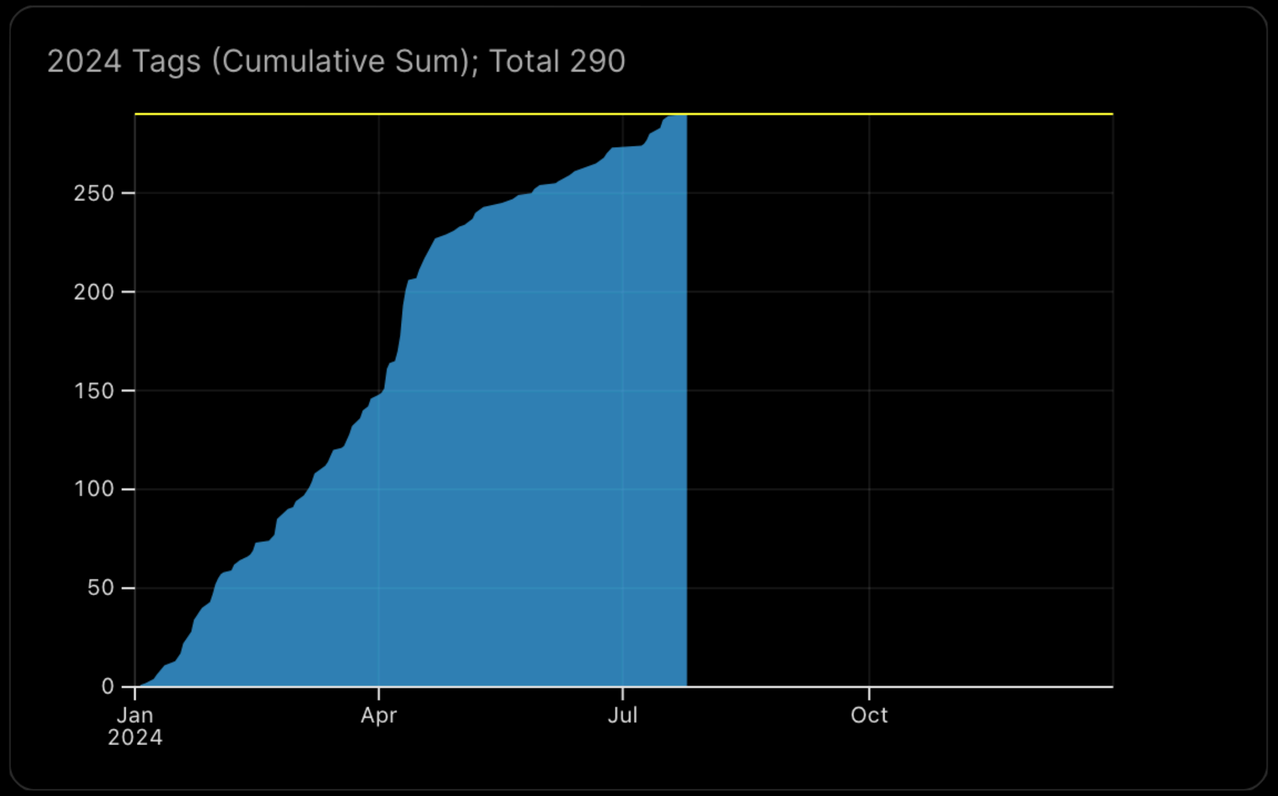
Security researchers have warned for years about industrial control systems (ICS) connected to the Internet. Reports on the number of devices speaking ICS protocols are often used to illustrate the severity of the problem. However, while there are indeed many ICS devices connected to the Internet, simply counting everything that looks like it may be ICS is not the most accurate method for measuring ICS exposure. There are many ICS honeypots that should be excluded from these types of analyses, which range from relatively easy to more challenging to detect. Moreover, many of the devices speaking these protocols aren't connected to critical infrastructure at all, but personal projects or lab setups. While large numbers make for click-worthy headlines, we strive to paint a measured yet comprehensive picture of real ICS device exposure on the Internet. In this talk, we'll discuss the analysis process from data collection to determining whether an ICS protocol is a "real" device, what these numbers mean in context, and why you really can't believe everything you see on the Internet.

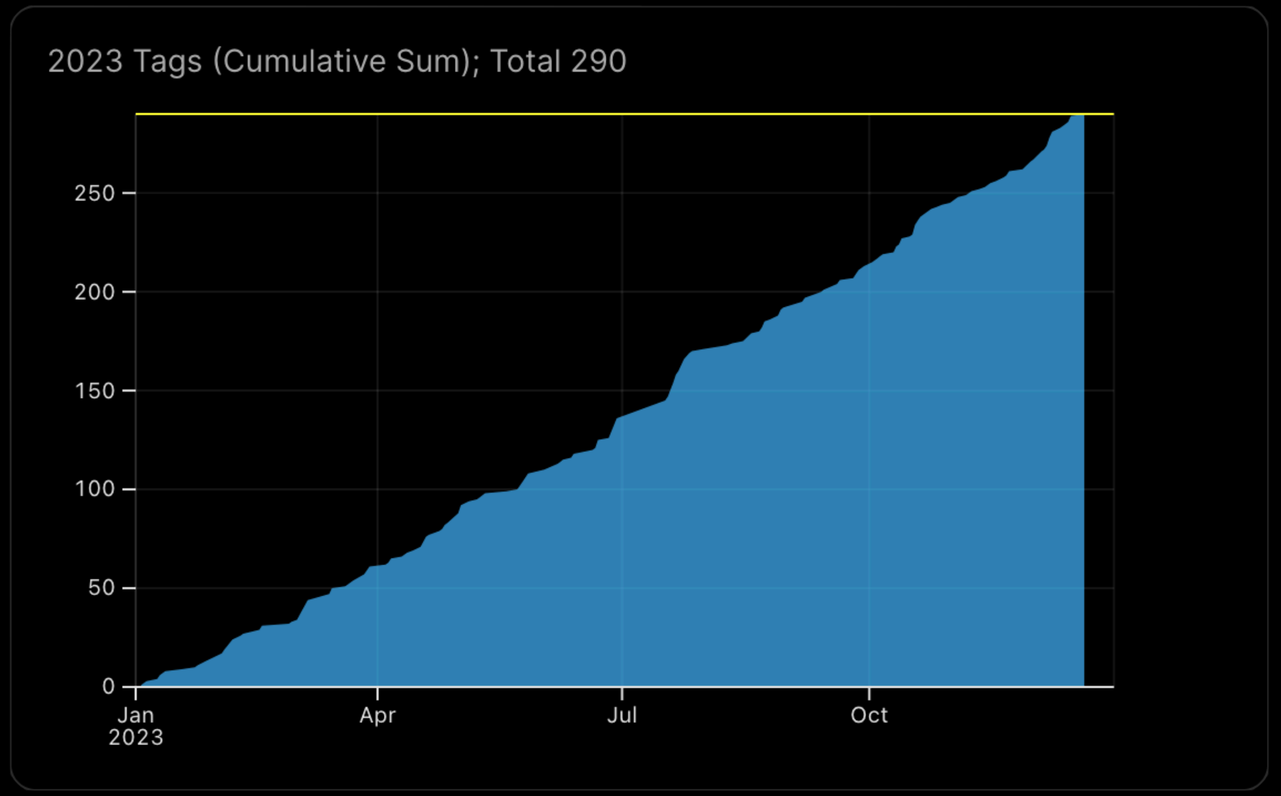
Emily Austin

STORM WATCH

CYBERSECURITY NEWS

TAG ROUND-UP


2024 Tags (Cumulative Sum); Total 290
250
200
150
100
50
0
Jan
2024
Apr
Jul
Oct


2023 Tags (Cumulative Sum); Total 290
250
200
150
100
50
0
Jan
2023
Apr
Jul
Oct

Ruijie RG-UAC CVE-2024-4813 RCE Attempt

WE NEED

TO TALK

ABOUT

KEV

STORM WATCH

It Has Been

1

Days Since The
Last KEV Release

https://kev.hrbrmstr.app

CVE-2024-39891: Twilio Authy Information Disclosure

CVE-2012-4792: Microsoft Internet Explorer Use-After-Free

CVE-2023-45249: Acronis Cyber Infrastructure (ACI) Insecure Default Password

CVE-2024-5217: ServiceNow Incomplete List of Disallowed Inputs

CVE-2024-4879: ServiceNow Improper Input Validation