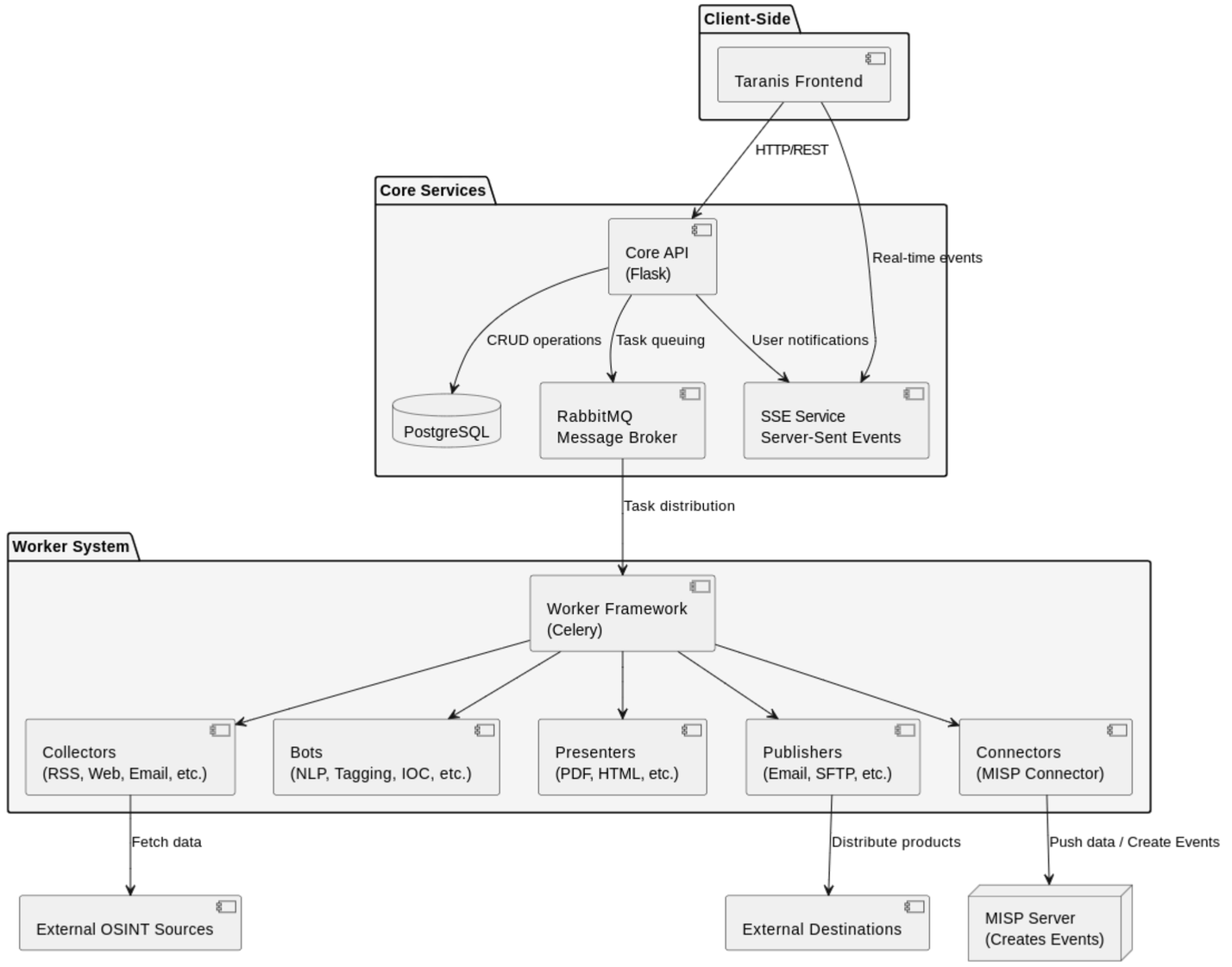
TARANIS AI

Taranis AI

taranis-ai/taranis-ai

Taranis System Architecture



Notable Features

Task queue via Celery for asynchronous news item processing

Modern NLP features like entity recognition and summary creation

Story clustering to reduce analyst workload

Keyword and tag dashboard visualization

Notable Features

Recognizes cybersecurity terms like APTs, CVEs, IoCs

Include/exclude lists for collection and tagging

Advanced search and filters for item management

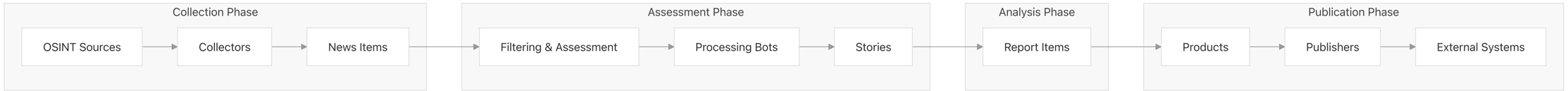
Grouped sources for easier task application

Collect Taranis collects data from various sources, including:

- **Websites** - News, blogs, forums
- **Social Media** - Twitter, Reddit, etc.
- **Dark Web** - Forums, marketplaces
- **Public Datasets** - CVE databases, APT reports

Assess - Taranis helps assess the relevance and reliability of the collected data:

- **Relevance** - How relevant is the data to your needs?
- **Reliability** - Is the source trustworthy?
- **Timeliness** - Is the information up-to-date?
- **Impact** - What is the potential impact of the information?


Collection Phase
OSINT Sources
Collectors
News Items
Assessment Phase
Filtering & Assessment
Processing Bots
Stories
Analysis Phase
Report Items
Publication Phase
Products
Publishers
External Systems

Analyze - Taranis analyzes the collected data to extract insights:

- **Named Entity Recognition (NER)** - Identifying entities like people, organizations, locations
- **Sentiment Analysis** - Understanding the sentiment of the text
- **Topic Modeling** - Discovering topics within the data
- **Trend Analysis** - Identifying trends over time

Publish - Taranis publishes the analyzed data in a user-friendly format:

- **PDF** - Reports with detailed analysis
- **HTML** - Interactive web pages
- **JSON** - Structured data for further processing

Published: 2024-10-25 22:22
2024-10-29 14:24 ⚠

Tags: Russia-linked, Android, Ukraine's, MeduzaStealer, PureStealer, UNC5812's, Russia's, Telegram, Russian-linked, Russia, Sunspinner, CraxsRAT, pro-Russian, UNC5812, Ukrainian, Visual Basic Script-based, HOMESTEEL, ClickFix-style, PowerShell, Windows, CERT-UA

Vote: 0 0

Article: darkreading.com

Angreifer nutzten gefälschte AWS-Domains in Phishingkampagne (7)

Angreifer nutzten gefälschte AWS-Domains in Phishingkampagne
AWS hat offenbar zahlreiche gefälschte AWS-Domains vom Netz genommen, die ukrainische Opfer auf Malware-Downloadseiten locken sollten.
- Kathrin Stoll
Sicherheitsforscher des AWS Security Team haben eine Phishing-Kampagne gestoppt, bei der tausende gefälschte AWS-Domains genutzt wurden. Amazon hat seit der Entdeckung der Kampagne massenweise Domains abgeschaltet. Die AWS-Sicherheitsforscher und das Computer Emergency Response Team der Uk
ukrainischsprachigen Zielen zu erbeuten.
Ukrainische Ziele im Visier
Die gefälschten AWS-URLs dienten offenbar als Köder. Nachdem die Opfer auf den Link einer solchen URL geklickt hatten, landeten sie auf einer Malware-Downloadseite, die einen sogenannten RDP-Trojaner installiert, der Anmeldedaten von Windows-Systemen stiehlt.
Amazons Chief Information Security Officer CJ Moses schrieb in einem Posting auf LinkedIn, dass Amazon selbst nicht im Visier der Angreifer war. Auch zielten die Angriffe nicht auf Anmeldedaten von AWS-Kunden ab. Stattdessen hatten die Angreifer Ziele mit Verbindungen zu Regierungsbehörden, Unternehmen und
enger gefassten Ansatz – dieses Mal seien die Phishingmails an viele Ziele verschickt worden.
Das ukrainische CERT hat ein Advisory mit weiteren Details zu dem Fall veröffentlicht. Cybercrime spielt im Krieg Russlands gegen die Ukraine auf beiden Seiten eine Rolle. Im Juni etwa machten die ukrainischen Behörden Personen dingfest, die sie der Cyberkriminalität verdächtigten, die mutmaßlich im Dienst russisc
(kst)

Published: Oct 28, 2024, 21:22:45
Article: darkreading.com
Author: Becky Bracken, Senior Editor, Dark Reading

Russia Kneecaps Ukraine Army Recruitment With Spoofed 'Civil Defense' App

Russia Kneecaps Ukraine Army Recruitment With Spoofed 'Civil Defense' App
Posing as an application used to locate Ukrainian military recruiters, a Kremlin-backed hacking initiative delivers malware, along with disinformation designed to undermine sign-ups for soldiers in the war against Russia.
October 28, 2024
Ukrainian efforts to recruit new soldiers to serve in its military in the country's war against Russia is under a two-pronged cyberattack by Kremlin-backed threat actors.
Researchers at Google's Threat Intelligence Group (TAG) and Mandiant have tracked down an active campaign that uses a spoofed version of the legitimate Ukrainian-language tool "Civil Defense," a crowdsourced mapping tool used to locate military recruiters. Attackers are using the fake version to perform dual malici
The hybrid op, which researchers named UNC5812, uses a Telegram channel to lure perspective recruits to a download the malicious version of "Civil Defense" from a spoofed site, outside of the confines of Google Play. Once downloaded, the application drops Windows and Android malware.
Russian Opp Uses Malware With a Side of Social Engineering
Windows users who make their way to the fake "Civil Defense" site to download the tool will be delivered the Pronsis Loader, which then starts a chain to deliver a malicious mapping application called Sunspinner, as well as an infostealer called Purestealer.
Android users, on the other hand, get a common user backdoor called Craxsrat, in addition to Sunspinner.
"Notably, the Civil Defense website also contains an unconventional form of social engineering designed to preempt user suspicions about APK delivery outside of the App Store and justify the extensive permissions required for the Craxsrat installation," the report noted. "The website's FAQ contains a strained justificatio
accompanying video instructions."
The video also provides instructions on how to disable Google Play Protect.
"While the Civil Defense website also advertises support for macOS and iPhones, only Windows and Android payloads were available at the time of analysis," the report said.
Sunspinner, a decoy graphical user interface (GUI) application written using the Flutter framework, offers functionality aimed to convince victims that the application is legitimate.
"Consistent with the functionality advertised on the [legitimate] Civil Defense website, Sunspinner is capable of displaying crowdsourced markers with the locations of the Ukrainian military recruiters, with an option for users to add their own markers," according to the Google TAG analysis. But the fake map offers only fak
inputs. All markers present [were pulled from the attacker's C2 and] were added on the same day by the same user."
Parallel Anti-Mobilization Effort Against Ukrainian Military
In tandem with the espionage effort, the other goal of the Russian fake Civil Defense campaign is to deliver disinformation aimed at suppressing Ukraine's military mobilization effort for the war. The malicious versions of Civil Defense's site and Telegram have pushed out videos with incendiary, anti-Ukrainian-military titles
Users who click on the button provided by the Russian hacker-operated site to "Send Material," ostensibly to discredit recruitment efforts, are automatically fed an attacker-controlled chat thread," the report said. "Anti-mobilization content cross-posted to the group's website and Telegram channel appears to be sourced fr
account."
Russia has consistently used cyberattacks as part of its war strategy against Ukraine, as well as against other governments, including a recent distributed denial-of-service (DDoS) cyberattack campaign against shipping ports in Japan. Russian hackers have also been working feverishly to distribute disinformation ahead
uncovered "Civilian Defense" campaign highlights, that's just one of many hacker groups doing the Kremlin's dirty work in cyberspace.
About the Author
You May Also Like

Published: Oct 25, 2024, 22:22:37
Article: darkreading.com
Author: Nate Nelson, Contributing Writer

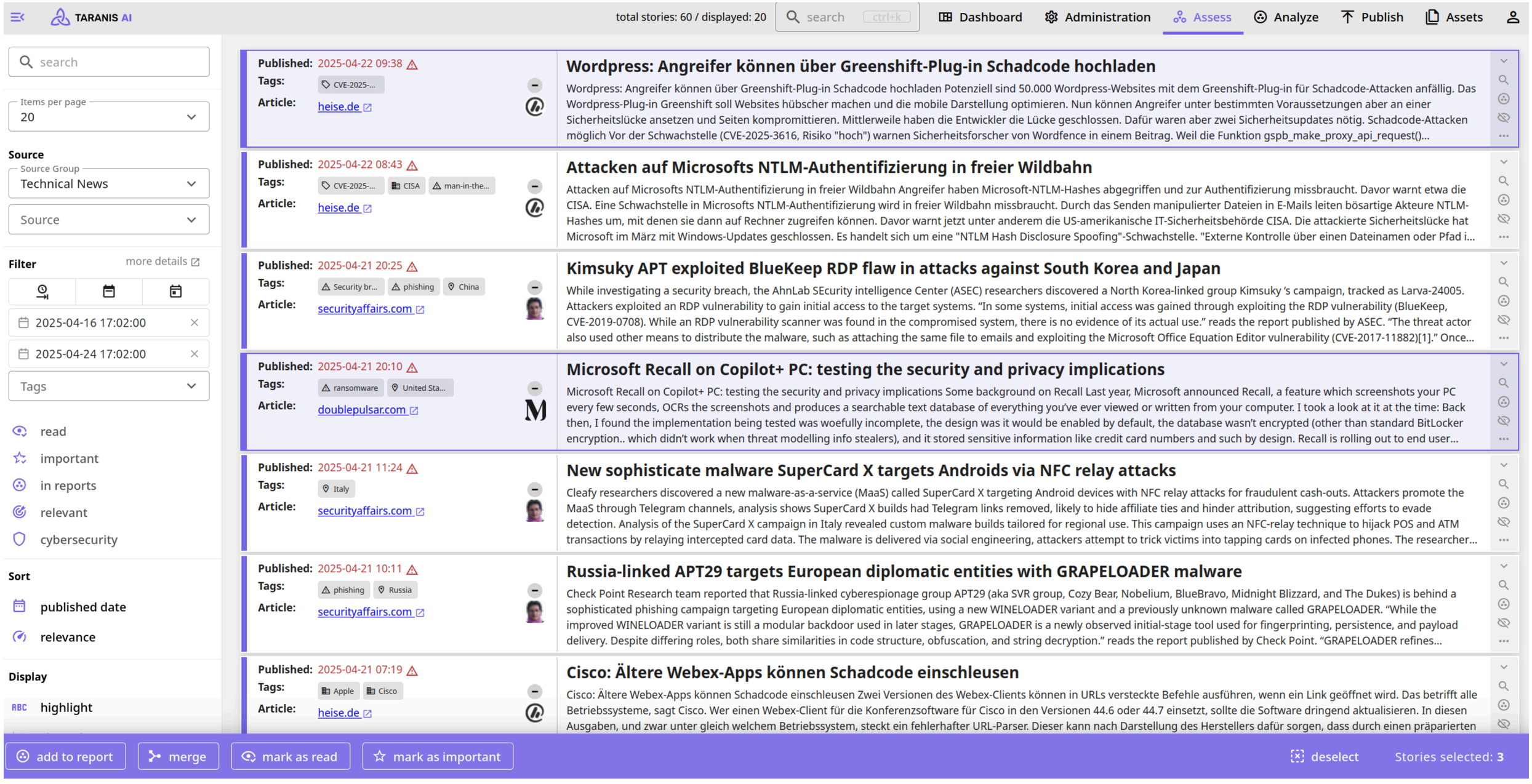
Russia's APT29 Mimics AWS Domains to Steal Windows Credentials

Russia's APT29 Mimics AWS Domains to Steal Windows Credentials
Kremlin intelligence carried out a wide-scale phishing campaign in contrast to its usual, more targeted operations.
October 25, 2024
Russia's premiere advanced persistent threat group has been phishing thousands of targets in militaries, public authorities, and enterprises.
APT29 (aka Midnight Blizzard, Nobelium, Cozy Bear) is arguably the world's most notorious threat actor. An arm of the Russian Federation's Foreign Intelligence Service (SVR), it's best known for the historic breaches of SolarWinds and the Democratic National Committee (DNC). Lately, it has breached Microsoft's codel
"APT29 embodies the 'persistent' part of 'advanced persistent threat,'" says Satnam Narang, senior staff research engineer at Tenable. "It has persistently targeted organizations in the United States and Europe for years, utilizing various techniques, including spear-phishing and exploitation of vulnerabilities to gain initial
future operations."
Along these same lines, the Computer Emergency Response Team of Ukraine (CERT-UA) recently discovered APT29 phishing Windows credentials from government, military, and private sector targets in Ukraine. And after comparing notes with authorities in other countries, CERT-UA found that the campaign was actua
That APT29 would go after sensitive credentials from geopolitically prominent and diverse organizations is no surprise, Narang notes, though he adds that "the one thing that does kind of stray from the path would be its broad targeting, versus [its typical more] narrowly focused attacks."
AWS and Microsoft
The campaign, which dates back to August, was carried out using malicious domain names designed to seem like they were associated with Amazon Web Services (AWS). The emails sent from these domains pretended to advise recipients on how to integrate AWS with Microsoft services, and how to implement zero tru
Despite the masquerade, AWS itself reported that the attackers weren't after Amazon, or its customers' AWS credentials.
What APT29 really wanted was revealed in the attachments to those emails: configuration files for Remote Desktop, Microsoft's application for implementing the Remote Desktop Protocol (RDP). RDP is a popular tool that legitimate users and hackers alike use to operate computers remotely.
"Normally, attackers will try to brute force their way into your system or exploit vulnerabilities, then have RDP configured. In this case, they're basically saying: 'We want to establish that connection [upfront].'" Narang says.
Launching one of these malicious attachments would have immediately triggered an outgoing RDP connection to an APT29 server. But that wasn't all: The files also contained a number of other malicious parameters, such that when a connection was made, the attacker was given access to the target computer's storage,
Block RDP
APT29 may not have used any legitimate AWS domains, but Amazon still managed to interrupt the campaign by seizing the group's malicious copycats.
For potential victims, CERT-UA recommends strict precautions: not just monitoring network logs for connections to IP addresses tied to APT29 but also analyzing all outgoing connections to all IP addresses on the wider Web through the end of the month.
And for organizations at risk in the future, Narang offers simpler advice. "First and foremost, don't allow RDP files to be received. You can block them at your email gateway. That's going to kneecap this whole thing," he says.
AWS declined to provide further comment for this story. Dark Reading has also reached out to Microsoft for its perspective.
About the Author
You May Also Like

Published: Oct 26, 2024, 11:36:00
Article: thehackernews.com
Author: info@thehackernews.com (The Hacker News)

CERT-UA Identifies Malicious RDP Files in Latest Attack on Ukrainian Entities

The Computer Emergency Response Team of Ukraine (CERT-UA) has detailed a new malicious email campaign targeting government agencies, enterprises, and military entities.
"The messages exploit the appeal of integrating popular services like Amazon or Microsoft and implementing a zero-trust architecture," CERT-UA said. "These emails contain attachments in the form of Remote Desktop Protocol ('.rdp') configuration files."
Once executed, the RDP files establish a connection with a remote server, enabling the threat actors to gain remote access to the compromised hosts, steal data, and plant additional malware for follow-on attacks.
Infrastructure preparation for the activity is believed to have been underway since at least August 2024, with the agency stating that it's likely to spill out of Ukraine to target other countries.
CERT-UA has attributed the campaign to a threat actor it tracks as UAC-0215. Amazon Web Service (AWS), in an advisory of its own, linked it to the Russian nation-state hacking group known as APT29.
"Some of the domain names they used tried to trick the targets into believing the domains were AWS domains (they were not), but Amazon wasn't the target, nor was the group after AWS customer credentials," CJ Moses, Amazon's chief information security officer, said. "Rather, APT29 sought its targets' Windows creder
The tech giant said it also seized the domains the adversary was using to impersonate AWS in order to neutralize the operation. Some of the domains used by APT29 are listed below -
- ca-west-1.mfa-gov[.]cloud
- central-2-aws.ua-aws[.]army
- us-east-2-aws.ua-gov[.]cloud

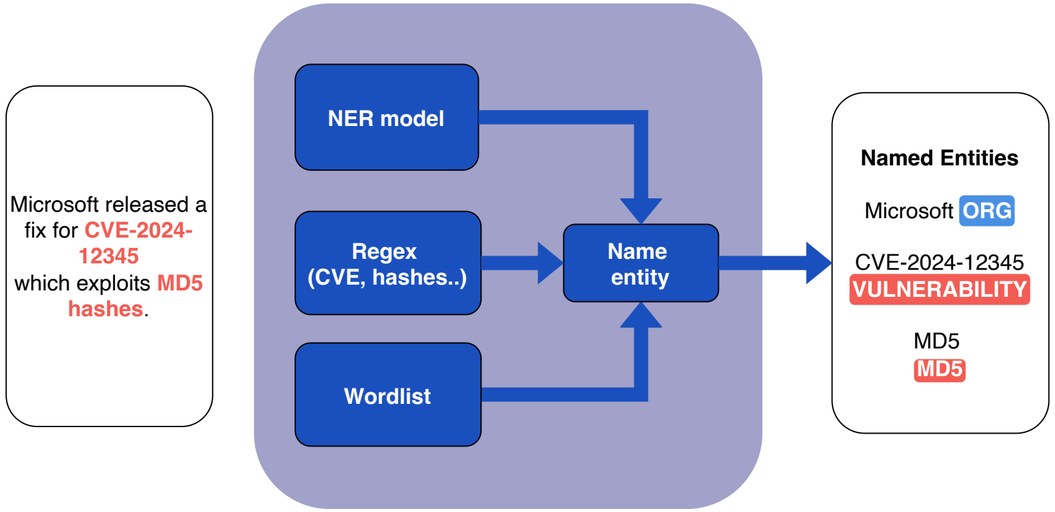

TARANIS AI
total stories: 60 / displayed: 20
search ctrl+k
Dashboard
Administration
Assess
Analyze
Publish
Assets
search
Items per page
20
Source
Source Group
Technical News
Source
Filter
more details
2025-04-16 17:02:00
2025-04-24 17:02:00
Tags
read
important
in reports
relevant
cybersecurity
Sort
published date
relevance
Display
highlight
Published: 2025-04-22 09:38
Tags: CVE-2025-...
Article: heise.de
Wordpress: Angreifer können über Greenshift-Plug-in Schadcode hochladen
Wordpress: Angreifer können über Greenshift-Plug-in Schadcode hochladen Potenziell sind 50.000 Wordpress-Websites mit dem Greenshift-Plug-in für Schadcode-Attacken anfällig. Das Wordpress-Plug-in Greenshift soll Websites hübscher machen und die mobile Darstellung optimieren. Nun können Angreifer unter bestimmten Voraussetzungen aber an einer Sicherheitslücke ansetzen und Seiten kompromittieren. Mittlerweile haben die Entwickler die Lücke geschlossen. Dafür waren aber zwei Sicherheitsupdates nötig. Schadcode-Attacken möglich Vor der Schwachstelle (CVE-2025-3616, Risiko "hoch") warnen Sicherheitsforscher von Wordfence in einem Beitrag. Weil die Funktion gspb_make_proxy_api_request()...
Published: 2025-04-22 08:43
Tags: CVE-2025-... CISA man-in-the...
Article: heise.de
Attacken auf Microsofts NTLM-Authentifizierung in freier Wildbahn
Attacken auf Microsofts NTLM-Authentifizierung in freier Wildbahn Angreifer haben Microsoft-NTLM-Hashes abgegriffen und zur Authentifizierung missbraucht. Davor warnt etwa die CISA. Eine Schwachstelle in Microsofts NTLM-Authentifizierung wird in freier Wildbahn missbraucht. Durch das Senden manipulierter Dateien in E-Mails leiten bösartige Akteure NTLM-Hashes um, mit denen sie dann auf Rechner zugreifen können. Davor warnt jetzt unter anderem die US-amerikanische IT-Sicherheitsbehörde CISA. Die attackierte Sicherheitslücke hat Microsoft im März mit Windows-Updates geschlossen. Es handelt sich um eine "NTLM Hash Disclosure Spoofing"-Schwachstelle. "Externe Kontrolle über einen Dateinamen oder Pfad i...
Published: 2025-04-21 20:25
Tags: Security br... phishing China
Article: securityaffairs.com
Kimsuky APT exploited BlueKeep RDP flaw in attacks against South Korea and Japan
While investigating a security breach, the AhnLab SEcurity intelligence Center (ASEC) researchers discovered a North Korea-linked group Kimsuky 's campaign, tracked as Larva-24005. Attackers exploited an RDP vulnerability to gain initial access to the target systems. "In some systems, initial access was gained through exploiting the RDP vulnerability (BlueKeep, CVE-2019-0708). While an RDP vulnerability scanner was found in the compromised system, there is no evidence of its actual use." reads the report published by ASEC. "The threat actor also used other means to distribute the malware, such as attaching the same file to emails and exploiting the Microsoft Office Equation Editor vulnerability (CVE-2017-11882)[1]." Once...
Published: 2025-04-21 20:10
Tags: ransomware United Sta...
Article: doublepulsar.com
Microsoft Recall on Copilot+ PC: testing the security and privacy implications
Microsoft Recall on Copilot+ PC: testing the security and privacy implications Some background on Recall Last year, Microsoft announced Recall, a feature which screenshots your PC every few seconds, OCRs the screenshots and produces a searchable text database of everything you've ever viewed or written from your computer. I took a look at it at the time: Back then, I found the implementation being tested was woefully incomplete, the design was it would be enabled by default, the database wasn't encrypted (other than standard BitLocker encryption.. which didn't work when threat modelling info stealers), and it stored sensitive information like credit card numbers and such by design. Recall is rolling out to end user...
Published: 2025-04-21 11:24
Tags: Italy
Article: securityaffairs.com
New sophisticate malware SuperCard X targets Androids via NFC relay attacks
Cleafy researchers discovered a new malware-as-a-service (MaaS) called SuperCard X targeting Android devices with NFC relay attacks for fraudulent cash-outs. Attackers promote the MaaS through Telegram channels, analysis shows SuperCard X builds had Telegram links removed, likely to hide affiliate ties and hinder attribution, suggesting efforts to evade detection. Analysis of the SuperCard X campaign in Italy revealed custom malware builds tailored for regional use. This campaign uses an NFC-relay technique to hijack POS and ATM transactions by relaying intercepted card data. The malware is delivered via social engineering, attackers attempt to trick victims into tapping cards on infected phones. The researcher...
Published: 2025-04-21 10:11
Tags: phishing Russia
Article: securityaffairs.com
Russia-linked APT29 targets European diplomatic entities with GRAPELOADER malware
Check Point Research team reported that Russia-linked cyberespionage group APT29 (aka SVR group, Cozy Bear, Nobelium, BlueBravo, Midnight Blizzard, and The Dukes) is behind a sophisticated phishing campaign targeting European diplomatic entities, using a new WINELOADER variant and a previously unknown malware called GRAPELOADER. "While the improved WINELOADER variant is still a modular backdoor used in later stages, GRAPELOADER is a newly observed initial-stage tool used for fingerprinting, persistence, and payload delivery. Despite differing roles, both share similarities in code structure, obfuscation, and string decryption." reads the report published by Check Point. "GRAPELOADER refines...
Published: 2025-04-21 07:19
Tags: Apple Cisco
Article: heise.de
Cisco: Ältere Webex-Apps können Schadcode einschleusen
Cisco: Ältere Webex-Apps können Schadcode einschleusen Zwei Versionen des Webex-Clients können in URLs versteckte Befehle ausführen, wenn ein Link geöffnet wird. Das betrifft alle Betriebssysteme, sagt Cisco. Wer einen Webex-Client für die Konferenzsoftware für Cisco in den Versionen 44.6 oder 44.7 einsetzt, sollte die Software dringend aktualisieren. In diesen Ausgaben, und zwar unter gleich welchem Betriebssystem, steckt ein fehlerhafter URL-Parser. Dieser kann nach Darstellung des Herstellers dafür sorgen, dass durch einen präparierten
add to report
merge
mark as read
mark as important
deselect
Stories selected: 3

NAMED ENTITY RECOGNITION

Locates and classifies entities

Beyond simple tagging

Enhances search precision


Microsoft released a fix for CVE-2024-12345 which exploits MD5 hashes.
NER model
Regex (CVE, hashes..)
Wordlist
Name entity
Named Entities
Microsoft ORG
CVE-2024-12345
VULNERABILITY
MD5
MD5

Summarization in OSINT Analysis

Streamlines analysis

Applies to news and stories

Facilitates report summaries

Future Directions

AI-assisted report templating

Learning from past reports

Entity Linking

LLM assisstant

Live Demo