Risky Biz News: US takes down RT's Twitter bot farm

By Catalin Cimpanu

Published: 2024-07-10 · Archived: 2026-04-02 11:24:14 UTC

This newsletter is brought to you by Devicie. You can subscribe to an audio version of this newsletter as a podcast by searching for "Risky Business News" in your podcatcher or subscribing via this RSS feed. On Apple Podcasts:

> Risky Business News: Risky Biz News: US takes down RT's Twitter bot farm on Apple Podcasts
>
> Show Risky Business News, Ep Risky Biz News: US takes down RT's Twitter bot farm - 9 July 2024

Apple Podcasts

The US Department of Justice has taken down a Twitter botnet operated by Russian news organization RT that was used to spread Kremlin propaganda on a large scale across Europe and the US.

According to court documents, the botnet consisted of at least 968 accounts and was operated by an editor-in-chief from RT's Moscow headquarters.

The botnet was established in early 2022, shortly after Russia's invasion of Ukraine, and its main role was to spread disinformation and favorable Russian narratives about the war.

According to a technical report [*PDF*] published by the FBI, RT used an AI tool named Meliorator to build and control the botnet's behavior.

This tool consists of two main components—Brigadir (frontend) and Taras (backend). From the FBI report:

> "*Brigadir serves as the primary end user interface of Meliorator and functions as the administrator panel. Brigadir serves as the graphical user interface for the Taras application and includes tabs for "souls," false identities that would create the basis for the bots, and "thoughts," which are the automated scenarios or actions that could be implemented on behalf of the bots, such as sharing content to social media in the future.*"

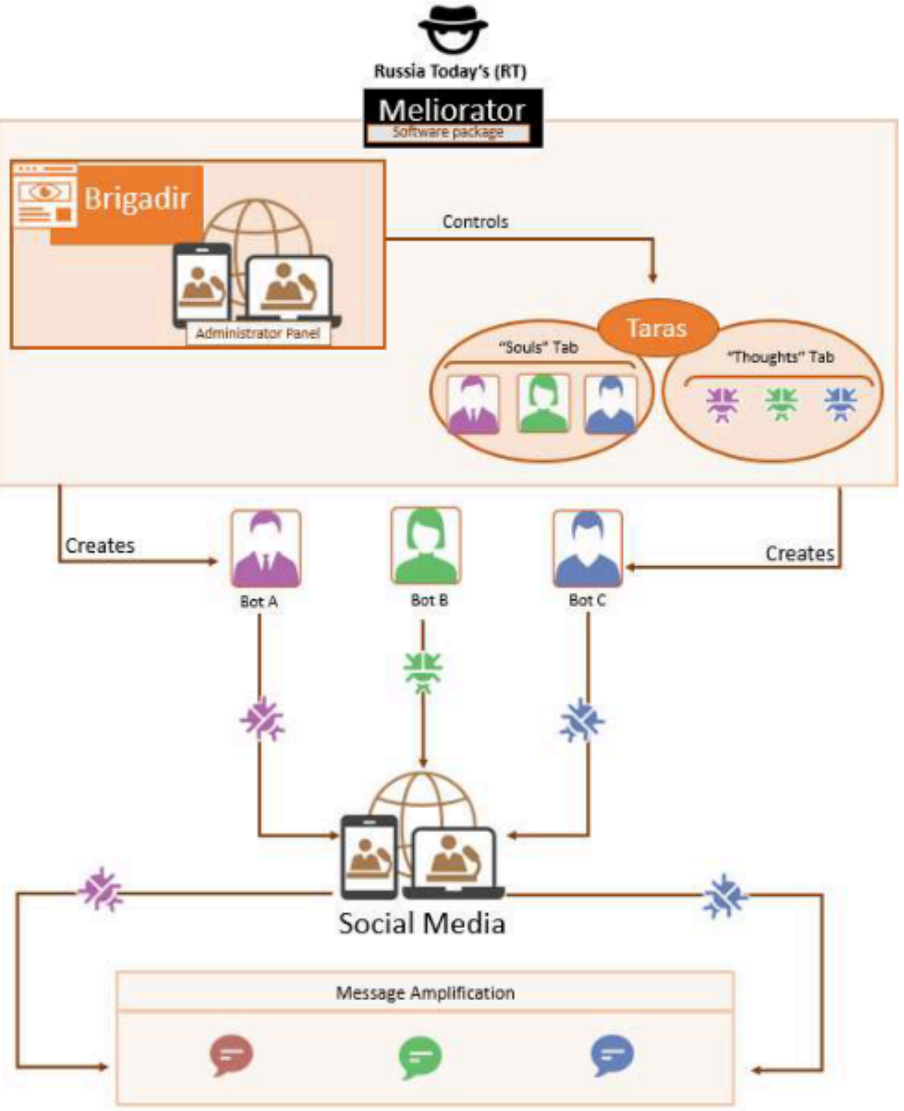


Figure 6: Technical Details Diagram

The botnet allowed operators to create fake online persons, register a Twitter account on their behalf, bypass Twitter verifications using an on-board email server, and configure campaigns on certain topics and with automated replies.

The bots were configured to take the identities of local citizens but would often post Russian propaganda and disinformation.

RT and its ilk used Meliorator to spread propaganda targeting audiences in the US, Poland, Germany, the Netherlands, Spain, Ukraine, and Israel.

The FBI says the tool was designed for use on Twitter, but it could have been easily adapted to other social networks as well.

The DOJ says it discovered the botnet after identifying Meliorator control panels operating on two domains, on mlrtr[.]com and otanmailp[.]com, both of which were registered with identities linked to the (yet unnamed) RT Moscow editor-in-chief.

The Justice Department says the narratives would often come from a private intelligence organization (PIO) controlled by a Russian FSB officer that was established with the approval and financial support of the Presidential Administration of Russia.

Both the RT editor-in-chief and the FSB officer had direct access to the Meliorator control panels, per the DOJ.

The DOJ praised Twitter (now X, but we're not calling it that since nobody calls it that) for its voluntary takedown of all bot accounts.

Breaches, hacks, and security incidents

Evolve hack update: American bank Evolve has posted an update on its recent breach and says that hackers have stolen the data of 7.6 million of its customers.

Heritage Foundation hack: Hacktivist group SiegedSec claims to have breached American right-wing think tank the Heritage Foundation. The organization is known for Project 2025, an authoritarian Christian nationalist plan to reform the US government. SiegedSec claims it has access to passwords, email inboxes, and the names of all the Foundation's members. The group has leaked some of the data and claims its hack is a response to the organization's anti-LGBTQ agenda.

Turkey DDoS attacks: Two hacktivist groups, LulzSec Black and Moroccan Soldiers, have launched DDoS attacks against Turkish organizations for the country's mistreatment of Syrians. [*Additional coverage in DailyDarkWeb*]

Fujitsu breach: Fujitsu has confirmed that customer data was stolen in a data breach it initially reported in March this year.

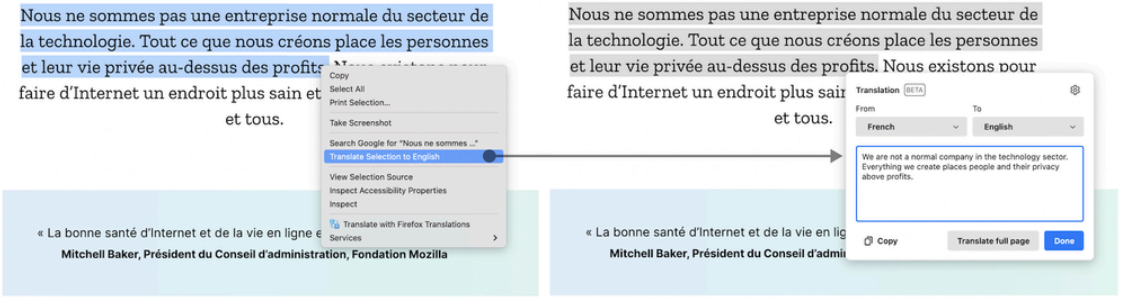
General tech and privacy

Firefox on Windows 7: Mozilla says it will extend support for Firefox on Windows 7. No new end-of-support was announced, but Mozilla was initially scheduled to drop Windows 7 support in September.

Notepad updates: Microsoft is rolling out support for spellcheck and autocorrect for the Notepad app on Windows 11, 40 years after the app's launch. [*Additional coverage in The Verge*]

Microsoft China blocks Android: Microsoft has mandated that all Chinese employees must use iPhones starting this September. The decision comes as the Google Play Store is blocked in China and employees can only install the Microsoft Authenticator app via the App Store. [*Additional coverage in BGR*]

Firefox 128: Mozilla has released Firefox 128. New features and security fixes are included. The biggest feature change in this release is the ability to translate pieces of text and a revamped UI for clearing cookies and past data.



Government, politics, and policy

CNMF's death: The Record's Martin Matishak looks at how Cyber Command is phasing out a CNMF project that shared malware samples on VirusTotal. The CNMF is now primarily focused on Under Assessment, a project between CyberCom and private security firms to share info about emerging threats via private channels like Slack and Microsoft Teams. [*This item has been edited post-publication due to an erroneous description.*]

AU assessment: The Australian government will run a stocktake of all its internet-facing systems and services by June next year. Government agencies will have to scan and determine what equipment and software they have exposed on the internet and from what software vendor or contractor. The end goal is to create a security risk management plan for all internet-facing systems or services. [*Additional coverage in itNews*]

Russian oppression database: The Russian government has built a database of all citizens who have fled the country after its invasion of Ukraine. The database is very likely being used for oppression purposes. The Kremlin previously used a leaked database of Navalny donors to fire government employees and detain individuals on charges of supporting terrorism. [*Additional coverage in The Agency*]

Russian censorship: Apple has removed 25 VPN apps from the Russian version of its App Store following a request from the country's telecommunications watchdog. The move comes after the Roskomnadzor has tried and failed to block VPN protocols at the network level for almost two years. Demand for VPN services soared in Russia after the country's invasion of Ukraine. [*Additional coverage in TechCrunch*]

In this Risky Business News sponsor interview, Catalin Cimpanu talks with Devicie Technical Product Manager Tom Plant on the upcoming Windows 10 end-of-support and the looming Great Windows 11 Migration.

Risky Business News: Sponsored: Devicie on the Great Windows 11 Enterprise Migration on Apple Podcasts

Show Risky Business News, Ep Sponsored: Devicie on the Great Windows 11 Enterprise Migration - 7 July 2024

Apple Podcasts

Cybercrime and threat intel

VasyGrek: Russian security firm FACCT has linked a malware developer known as Mr.Burns to a 38-year-old Ukrainian national. FACCT claims Andrey R. from the city of Ternopil has been involved in cybercrime since 2010 and is the author and seller of the Burns remote access trojan. The company says the BurnsRAT is a tool commonly used by VasyGrek, a cybercrime group that has been attacking Russian companies since at least 2020.

Crypto-drainers: If you're still confused about crypto-drainers and what they are (phishing kits specialized in targeting and automatically emptying crypto-wallets), then Cisco Talos has you covered.

Threat/trend reports: Cloudflare and Orange have recently published reports covering infosec industry threats and trends.

Malware technical reports

DoNeX ransomware: Security firm Avast has been secretly working with law enforcement authorities to provide free decrypters for victims of the DoNeX ransomware gang. Avast says it built the decrypter in March after its researchers found a flaw in the ransomware's cryptographic scheme. The company revealed its decrypter after

details of the same flaw were disclosed at a recent security conference. The decrypter works on users infected by the DoNeX ransomware, as well as previous versions known as DarkRace and Muse.

Coyote: BlackBerry has published a report on Coyote, a new banking trojan spotted earlier this year that primarily targets Brazilian financial institutions.

SilverFox: KnownSec404 has published a report on SilverFox, a Windows trojan primarily active in China. The Chinese security firm appears to believe the trojan is the work of an APT group that's trying to hide its espionage activities behind a cybercrime operation. It doesn't expand on the subject.

Kematian-Stealer: CyFirma has discovered a new infostealer named Kematian-Stealer that is available as a free tool on GitHub and has been recently seen in the wild.

APTs, cyber-espionage, and info-ops

APT40: Australia's cybersecurity agency has published a report and IOCs from two recent APT40 intrusions. The report marks the first time Australia has led the publishing and exposing of a Chinese APT's ops as part of a joint effort with other agencies abroad.

> *"The activity and techniques overlaps with the groups tracked as Advanced Persistent Threat (APT) 40, Kryptonite Panda, GINGHAM TYPHOON, Leviathan and Bronze Mohawk in industry reporting. This group has previously been reported as being based in Haikou, Hainan Province, PRC and receiving tasking from the PRC MSS, Hainan State Security Department."*

CloudSorcerer: Kaspersky has discovered a new APT group targeting Russian government entities. The new CloudSorcerer group has been active since May this year. Its main tool is a sophisticated toolkit designed to control malware implants and exfil data via Microsoft Graph, Yandex Cloud, and Dropbox cloud infrastructure. Kaspersky did not link the group to any state. Proofpoint says it spotted the same group also targeting US think tanks.

Lifting Zmiy: Rostelecom's security team has discovered a new APT group that is breaching companies via industrial PLCs. Named Lifting Zmiy, the group's first attacks were traced back to October of last year. The group targeted PLCs from Russian company Tech-Automatics usually used with elevators and which were still using

their default passwords. Rostelecom has linked the group to intrusions at a Russian government contractor, two telecom operators, and an IT company. The company says the group collected and exfiltrated data and then destroyed the victim's infrastructure. Rostelecom says Lifting Zmiy uses Starlink infrastructure for attacks and appears to operate out of Ukraine.

Kimsuky: Japan's CERT team has published a report looking at Kimsuky operations targeting Japanese organizations.

DPRK npm malware: DevSecOps company Phylum has found another malicious JS library published on the npm portal by North Korean hackers. This one tried to pass as call-bind is a legitimate npm package with over 2,000 downstream dependents and over 45 million weekly downloads.

Houthi cyber ops, part I: Hackers linked with Houthi rebels have used spyware to target militaries across the Middle East since 2019. The attacks used a novel spyware strain named GuardZoo to collect photos and documents from infected devices. Targets included militaries in seven Middle East countries, such as Saudi Arabia, Oman, and Egypt. Security firm Lookout spotted the infections after it discovered a GuardZoo command and control server exposed online.

Houthi cyber ops, part II: On the same note, another Houthi-linked cyber group named OilAlpha has continued to use malicious mobile apps to target humanitarian and human rights organizations operating in Yemen. This is a continuation of a campaign that was first spotted last year.

Vulnerabilities, security research, and bug bounty

Patch Tuesday: Yesterday was the July 2024 Patch Tuesday. We had security updates from Adobe, Microsoft, Firefox, Cisco, Fortinet, SAP, Citrix [1, 2], Kubernetes, Schneider Electric, Siemens, and Zoom. The Android Project, VMWare, Elastic, Splunk, Apache HTTPD, and Mastodon released security updates last week as well. This month, Microsoft patched 142 vulnerabilities, including two zero-days. They include:

- CVE-2024-38080 — Windows Hyper-V Elevation of Privilege Vulnerability.
- CVE-2024-38112 — Windows MSHTML Platform Spoofing Vulnerability.

New Adobe Reader zero-day: Adobe is scheduled to release a patch for an Adobe Reader zero-day in August during its regular Patch Tuesday security updates. The zero-day was discovered [*archived*] by security researcher Haifei Li while scanning public PDF files for potential exploit code. Li says the exploit is unfinished and doesn't deliver a final payload.

Ghostscript exploitation: Threat actors are now exploiting a recently disclosed Ghostscript RCE (CVE-2024-29510) in the wild.

WhatsUp Gold RCE: Security researchers from the Summoning Team have published details and a PoC for an unauth RCE in the Progress Software WhatsUp Gold network monitoring solution. The bug is tracked as CVE-2024-4885. [*h/t ScreamingGoat*]

Splunk PoC: Security researcher Mohamed Nabil Ali has published a PoC for CVE-2024-36991, a path traversal in the Splunk SIEM.

Blast-RADIUS attack: A team of academics has developed a new attack that breaks the RADIUS authentication and authorization protocol. The new attack is named Blast-RADIUS and allows threat actors to convert failed authentication attempts into successful logins and access protected resources. The attack leverages a novel MD5 collision technique and requires a MitM position between RADIUS clients and servers. The RADIUS protocol was developed in the 1990s and is still in use today for protecting networking devices, mobile networks, and industrial equipment.

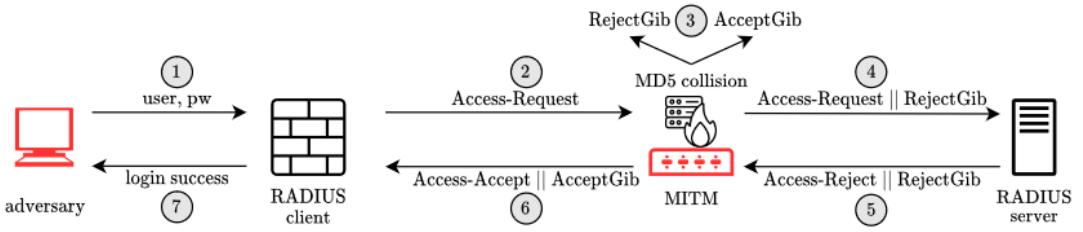


Figure 1: **Our attack flow.** Our adversary triggers an Access-Request with incorrect credentials from a legitimate RADIUS client (1), and then carries out a man-in-the-middle attack (2) and computes an MD5 hash collision (3) to inject a malicious Proxy-State attribute in the request (4). The hash collision allows the attacker to transfer the server-generated Response Authenticator from the legitimate Access-Reject response (5) to the attacker's desired Access-Accept response (6) to get authenticated or authorized by the RADIUS client (7).

Infosec industry

New tool—Incidental: A cool infosec project that has gone open-source recently is Incidental, a platform for managing your incidents within Slack. Still in early stages of development, though.

New tool—View8: Check Point has open-sourced View8, a static analysis tool designed to decompile serialized V8 bytecode objects (JSC files) into high-level readable code.

New tool—Flow Analyzer: Microsoft's Manuel Berrueta has open-sourced Flow Analyzer, a tool for helping in low level understanding and testing of OAuth 2.0 Grants/Flows.

New tool—Atom Ducky: Polish security researcher Flock4h has released Atom Ducky, a tool designed to work as a wirelessly operated Rubber Ducky, personal authenticator, and casual keyboard.

New tool—MailGoose: CERT-PL has open-sourced MailGoose, a tool that allows server admins to check whether their SPF, DMARC, and DKIM configuration is set up correctly.

Domain: cert.pl - e-mail sender verification mechanisms check results: SPF and DMARC

Check date: 2024-01-09 14:23:34.

If you want to share check results, copy the following link:

✓ Check summary: 2 mechanisms out of 2 configured without issues.

✓ SPF: correct configuration

Domain	cert.pl
Record	v=spf1 include:_spf.cert.pl -all
Warnings	none
Errors	none

✓ DMARC: correct configuration

Domain	cert.pl
Record	v=DMARC1; p=reject; rua=mailto:dmarc-cert@cert.pl; ruf=mailto:security@cert.pl; fo=s
Warnings	none
Errors	none

BSidesSF 2024 videos: Talks from the BSides San Francisco 2024 security conference, which took place in May, are now available on YouTube.

Risky Business Podcasts

In this edition of Between Two Nerds, Tom Uren and The Grugq talk about how bureaucracies should deal with outstandingly talented individuals.

In this podcast, Tom Uren and Patrick Gray talk about how South Korean internet regulations inadvertently encouraged a large ISP to hack their own customers to cut down on torrent traffic.

Abhishek Agrawal is the CEO and co-founder of Material Security, an email security company that locks down cloud email archives. Attackers have been raiding mailspools since hacking has existed, and with those mailspools now in the cloud with services like o365 and Google Workspace, guess where the attackers are going?
