< BACK TO BLOG

Mapping MITRE ATT&CK to SandWorm APT's Global Campaign

ABBY THURMAN 28 OCTOBER 2020

RELIAQUEST

On Thursday, October 15th, the United States Department of Justice (DoJ) indicted six Russian military officers connected to the SandWorm advanced persistent threat (APT) group, a threat group attributed to Russia's Main Intelligence Directorate (GRU). The indictment alleged that the men belonged to Military Unit 77445 of the GRU and coordinated a destructive cyber campaign against thousands of US and international corporations, organizations, political campaigns, and governments. The military officers purportedly conspired for Russia's strategic benefit through unauthorized access to victim computers to support broader Russian government efforts.

Abby Thurman

Content Marketing Strategist

Abby is a content strategist specializing in tech. She's passionate about translating difficult concepts into clear language. When she's not working, she's exploring Utah landscapes, reading, or hanging out with her pets.

Explore Blogs

Throughout the years, Digital Shadows (now ReliaQuest) has followed SandWorm, and we even analyzed the impact of the indictment in our recent ShadowTalk podcast. With this new indictment and a couple of new pieces of information, we thought this would be the perfect opportunity to revisit the tactics, techniques, and procedures (TTPs) behind the SandWorm APT.

A Brief Snapshot of SandWorm Threat Actors

SandWorm is an APT group that has been active since at least 2009, with some researchers suggesting the group was involved in attacks against Georgia in 2008. The tactics employed in SandWorm's campaigns align with GRU's philosophy of leveraging aggressive and sometimes destructive cyberattacks. The charges filed against SandWorm represent not only the first criminal charges against SandWorm for its most destructive attacks but the first time that most of the charged threat actors have been publicly identified as members of the cybercriminal group. They also represent SandWorm's first global law enforcement reaction to their deployment of the NotPetya malware, which crippled networks worldwide.

According to the Government Communications Headquarters (GCHQ), Russia is assessed as a highly competent threat actor with demonstrated potential to

carry out operations that have a myriad of impacts across any industry. Russia has been carrying out disruptive cyber activities to establish itself forcefully in various ways, including seeking to disrupt other countries' elections. For example, it has been widely reported that Russian state-associated groups were behind the "hack and leak" cyberattack, which aimed to breach French political party members' accounts in the run-up to the 2017 French elections.

The United Kingdom's Secret Intelligence Service (SIS) reported that this activity "comes to the very muddy nexus between business and corruption and state power in Russia." GCHQ also stated a "considerable balance of intelligence now which shows the links between serious and organized crime groups and Russian state activity."

Notable Campaigns Attributed to SandWorm

_ Around December 2015 and December 2016, SandWorm attempted to destabilize Ukraine by launching cyberattacks against companies that support the country's electric infrastructure, disrupting the supply of electricity to more than 225,000 Ukrainian customers.

_ SandWorm launched spearphishing campaigns targeting local government entities, political parties, and campaigns in France, including those connected with French President Emmanuel Macron's presidential campaign.

_ Around June 2017, SandWorm launched its "NotPetya" malware campaign, causing hundreds of victim organizations worldwide to lose one billion dollars collectively.

_ SandWorm retaliated against the 2018 Winter Olympics by launching cyberattacks against critical infrastructure after a Russian government-sponsored doping effort led to Russian athletes being unable to participate under the Russian flag.

_ Around April 2018, SandWorm undermined efforts to hold Russia accountable for its use of a weapons-grade nerve agent on foreign soil by launching spearphishing campaigns against international and government organizations investigating the poisoning of a former GRU officer and his daughter.

_ SandWorm defaced approximately 15,000 websites in Georgia by launching a cyberattack around October 2019.

MITRE ATT&CK Mapping

INITIAL ACCESS

T1566: Phishing

SandWorm threat group members primarily used spearphishing emails to gain access to computers or account credentials. The group specifically crafted the emails to resemble those from trustworthy or familiar senders. Attackers went so far as to develop and test spearphishing techniques before carrying out their campaigns to increase their success chances.

EXECUTION

T1059: Command and Scripting Interpreter

SandWorm heavily leveraged PowerShell

commands and scripts to discover system information, execute code, and download malware. In one instance, the group executed a malicious PowerShell script that contained versions of a credential harvesting tool. The tool operated only in memory and was not easily detectable by antivirus software.

T1204: User Execution

Many of the spearphishing emails sent by SandWorm contained malware-laced documents that required user execution to deploy.

PERSISTENCE

T1078: Valid Accounts

To maintain their foothold, SandWorm obtained and repeatedly used existing accounts' credentials to preserve persistence in victim systems. The group primarily deployed malware and leveraged hacking tools to maintain control over victim computers and networks.

PRIVILEGE ESCALATION

T1078: Valid Accounts

SandWorm leveraged malware to escalate system privileges and determine whether particular antivirus processors were running,

then attempted to identify other computers on the same network to potentially compromise.

DEFENSE EVASION

T1070: Indicator Removal on Host

SandWorm used an algorithm to obscure particular features of the Olympic Destroyer malware to obstruct post-attack investigations and avoid detection. The group also attempted to obfuscate their activity by deleting data from compromised machines and servers and clearing event logs.

T1036: Masquerading

On multiple occasions, SandWorm attempted to masquerade their activity through researching and emulating malware used by the Lazarus Group.

CREDENTIAL ACCESS

T1003: OS Credential Dumping

SandWorm dumped credentials to obtain account login and credential details from compromised machines.

T1552: Unsecured Credentials

SandWorm leveraged customized malware to overwrite itself to incorporate any additional

usernames and passwords that it could obtain from the previous computer before spreading to the next computer.

DISCOVERY

T1083: File and Directory Discovery

SandWorm repeatedly accessed and browsed files, ran malicious scripts, and searched compromised machines for credential files and files containing network configuration details.

LATERAL MOVEMENT

T1210: Exploitation of Remote Services

SandWorm exploited remote services to gain unauthorized access to internal systems. Once they gained access to the remote system, they deployed malware that was leveraged to obtain system privileges, extract and execute an open-source credential harvesting tool, and move laterally throughout the network.

COLLECTION

T1083: File and Directory Discovery

After gaining access to victims' computers, SandWorm threat actors performed various functions designed to identify, collect,

package, and view targeted data, including usernames, IP addresses, and server data relating to RDP sessions on the target computers. This activity included stealing credentials that allowed them to move laterally and exponentially throughout victims' computer networks.

COMMAND AND CONTROL

T1001: Data Obfuscation

SandWorm established command and control to create a single point of access between compromised networks and a server they controlled. The tunnel allowed them to hide their activity, issue commands, install additional tools, and transfer data.

EXFILTRATION

T1078: Valid Accounts

SandWorm leveraged legitimate credentials to exfiltrate data from a victim network and retrieve internal documents from machines

inside victim environments.

IMPACT

T1491: Defacement

SandWorm defaced approximately 1,500 websites and disrupted service to some of those websites following the Georgian web hosting provider's compromise.

T1490: Inhibit System Recovery

The group deployed destructive malware to delete files from the hard drive, force shutdowns, and impede rebooting and recovery by misconfiguring BitLocker, rendering computers inoperable.

What Can We Expect from This?

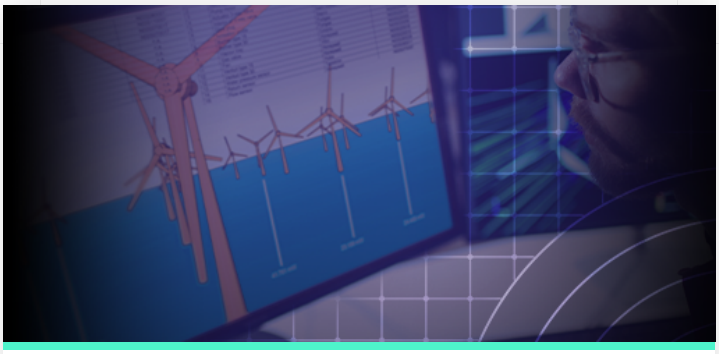
Considering the Russian Main Intelligence Directorate (GRU) allegedly sponsored SandWorm, its members' arrest and extraction are unlikely. However, it is possible that authorities would impose sanctions against the alleged cybercriminals and the GRU unit that sponsors them, considering this countermeasure has previously been used. For now, SandWorm's indictments will limit their ability to use the Western financial system or travel to any country that may have an extradition agreement with the US.

Is this indictment to deter future activity from Russia state-associated threat actors? Perhaps not, but it is a step in the right direction. Generally speaking, this will remind

threat actors that cyberattacks will not occur without consequences. As nation-state operations are investigated and pieced together through international cooperation, the US will likely continue to file indictments against associated actors to increase pressure on them.

RESOURCES

Related Blogs



RELIAQUEST

Report Reveals Spearphishing Constitutes 81% of Utilities Sector Alerts

1 MINS

RELIAQUEST | SECURITY OPERATIONS PLATFORM

Announcing the GreyMatter Notification Center

1 MINS

All Blogs

See **GreyMatter** in Action

Get a live demo of our security operations platform, GreyMatter, and learn how you can improve visibility, reduce complexity, and manage risk in your organization.

Request A Demo

Contact ReliaQuest Sales

(800) 925-2159

Global Corporate Headquarters
1001 Water St
Suite 1900
Tampa, FL 33602

Stay Ahead of Threats

Subscribe now to get updates on the latest emerging threats and industry trends in SecOps.

Sign Up

Unify Security Operations

- Solution Overview
- Reduce Noise and False Positives
- Automate Security Operations
- Dark Web Monitoring
- Maximize Security Investments
- Beyond MDR
- Secure Multi-Cloud Environments
- Secure Mergers and Acquisitions
- Operational Technology

Why ReliaQuest

- Explore the GreyMatter Platform
- Detection Investigation Response
- Threat Hunting
- Threat Intelligence
- Model Index
- Automated Response Playbooks
- Breach and Attack Simulation
- Digital Risk Protection
- Phishing Analyzer
- Technology Partners

Learn

- Resource Center
- Blog
- Threat Research
- Case Studies
- Data Sheets
- eBooks
- Industry Guides
- Research Reports
- ShadowTalk Podcast
- Solution Briefs
- White Papers
- Videos
- Events & Webinars

Company

- About ReliaQuest
- Leadership
- No Show Dogs Podcast
- Make It Possible in the Community
- Careers
- Press and Media Coverage
- Become a Technology Partner
- Contact Us
- Report a Vulnerability