Gamaredon Group: Understanding the Russian APT

threatstop.com/blog/gamaredon-group-understanding-the-russian-apt

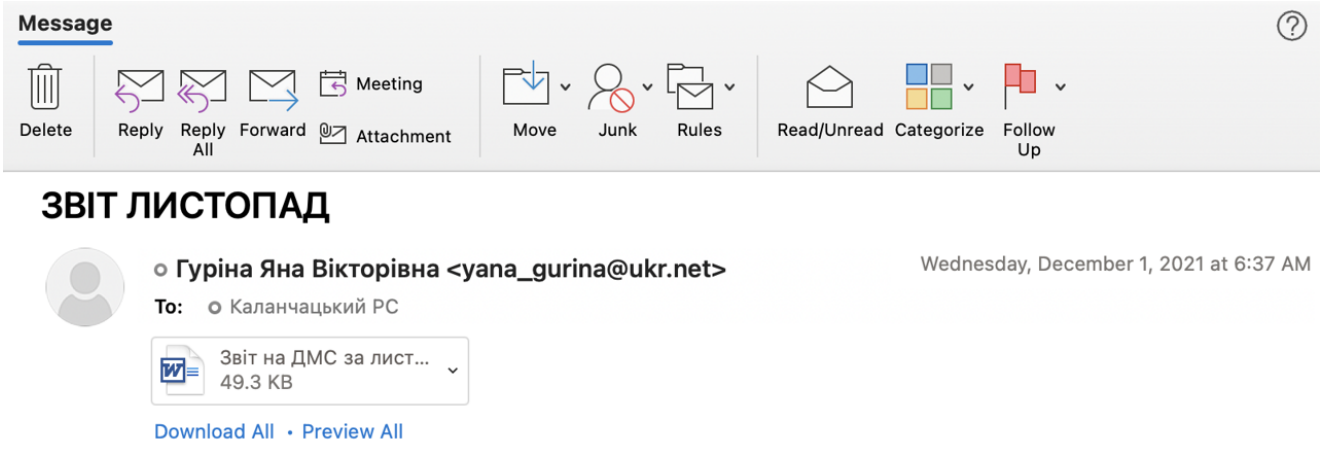
Our researchers have been following the Gamaredon Group (aka Primitive Bear) for years now, but ever since the Russo-Ukraine war broke out - they've been more relevant than ever. January 14, 2022 marked the first Russian cyber-war move, when a series of reports were published claiming Russian cyber attacks on the Ukrainian government - numerous government websites taken down or defaced, various targeted attacks using WhisperGate on Ukrainian organizations, and more. Since then, Russia has been playing hard in the cyber battlefield - and Gamaredon is a lead player.

Who is the Gamaredon Group

The Gamaredon Group has been active since at least 2013, not long before Russia annexed the Crimean peninsula. Over the years, speculations about their primary motives have been confirmed, with security researchers seeing multiple attacks targeting Ukrainian government organizations and officials. Last year, the Security Service of Ukraine (SSU) publicly attributed the adversary to five Russian Federal Security Service (FSB) officers posted in Crimea. The SSU has also claimed that Gamaredon is capable of surpassing extremely successful Russian APTs like APT28 (Sofacy/Fancy Bear), SNAKE (Turla), and APT29 (Cozy Bear/The Dukes) in the scale of their attacks and damage.

Infection Tactics

Gamaredon usually leverages email spear phishing using malicious office file attachments to infect their victims. But that's not all - the APT has a few creative tricks up its sleeve. Once example is their campaign targeting a Western government entity. Instead of the classic email phish, they played out a meticulous, precise attack by submitting a malicious downloader camouflaged as a CV onto a job search platform.



Email sent to a Ukranian government inbox. Image: Unit42

Once the malicious file is opened by the victim, a remote template injection technique is set in action. allowing the file to pull a malicious VBS script. The script then checks in with the APT's command and control (C2) servers, and after a wait period (6 hours for example), it

will pull a SelF-eXtracting (SFX) archive - one of Gamaredon's signature moves. The threat actor has been spotted using this tactic to bundle in evasive remote access persistence tools to victims machines for years. Today, Gamaredon uses UltraVNC, which gives the C2 server control of the compromised system. VBS files are also usually bundled in the payload, and a custom Gamaredon malware is downloaded.

Malware Variants

Different Gamaredon attacks have used different malware variants over time. For many years now, the threat actor has been using their own custom-created malware variants. PowerPunch is Gamaredon's droppers and downloader family, which shares it's evasiveness characteristic with Pterodo. The backdoor uses various obfuscation techniques, while giving the attackers interactive access to the network so they can carry out their attack plans. QuietSieve, another custom malware, steals information from the target host such as *doc*, *docx*, *xls*, rtf, odt, txt, jpg, pdf, rar, zip and 7z files, as well as screenshots taken by the malware. Other malware families employed by Gamaredon include ObfuMerry, ObfuBerry, DilongTrash, DinoTrain, and DesertDown.

Infrastructure

Gamaredon has been seen changing infrastructure over time. Analyzing hundreds of IOCs used by the APT in the past and present, it's clear that their favorite registrar by a landslide has always been REG-RU. Recently, Cisco released a table mapping the different IP spaces heavily associated with Gamaredon infrastructure.

Owner	ASN	Popular Networks	Distribution
REG.RU, Ltd	AS197695	194.67.71.0/24 194.67.112.0/24 194.58.100.0/24 194.58.112.0/24 194.58.92.0/24 89.108.81.0/24	45.93%
TimeWeb Ltd.	AS9123	185.104.114.0/24 188.225.77.0/24 188.225.82.0/24 94.228.120.0/24 94.228.123.0/24	28.25%
EuroByte LLC	AS210079	95.183.12.42/32	10.56%
AS-CHOOPA	AS20473	139.180.196.149/32	5.08%
LLC Baxet	AS51659	45.135.134.139/32 91.229.91.124/32	2.23%
System Service Ltd.	AS50448	109.95.211.0/24	1.82%

Distribution of Gamaredon-related IP addresses per ASN and owner. Image: Cisco

By integrating over 900 different threat intelligence feeds, ThreatSTOP provides comprehensive coverage of Gamaredon IOCs for optimum protection. As new IOCs are discovered, they are swiftly added to our system and propagated to blocklists and policies on all ThreatSTOP-protected networks. Our Core Threats IP and domain bundles allow customers to block thousands of Gamaredon infrastructure IOCs, including the related REG-

RU IP address spaces. Users who want to block Russia as a whole, not only by geo-blocking Russia, but also Crimea, Luhansk and Donetsk, and by blocking sanctioned Russian-related entities, can do so with our Russia Related bundles.