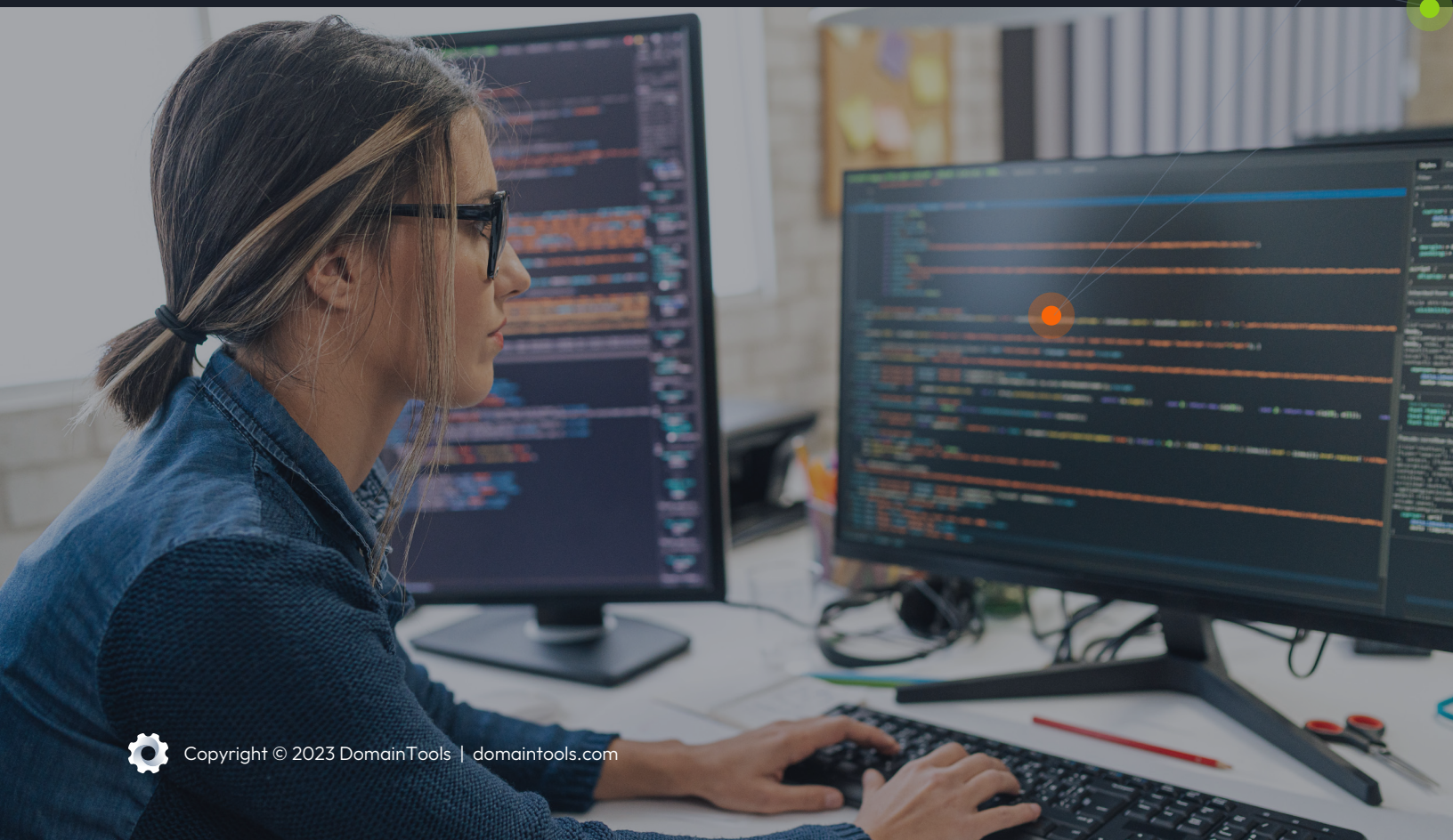
DomainTools

FARSIGHT SECURITY
A DOMAINTOOLS COMPANY

Walk on the Wild Side: Get to Know Cozy Bear



Overview

Cozy Bear, more officially classified as the Advanced Persistent Threat (APT) group 29, "APT29," is a Russian-based hacker group believed to be associated with Russia's foreign intelligence service. The group is also known under the nicknames Office Monkeys, CozyCar, The Dukes, and CozyDuke.

Kaspersky and CrySyS Lab researchers first reported on the group in July 2013, even though malicious activity had been previously observed but not yet attributed to a single group. As it turns out, APT29 has been actively engaging in cyber espionage activity since 2008, primarily targeting government entities and organizations involved in geopolitical affairs.

Over the past decade, APT29 continues to maintain its reputation as one of the most sophisticated APT groups out there. They have launched numerous destructive campaigns that distribute advanced malware to targets worldwide. Most recently, the widely-reported SolarWinds compromise has been attributed to the group.

2008

The first known targets of APT29's earliestdetected malware, PinchDuke, were associated with the Chechen separatist movement. The delivery mechanisms were malicious Microsoft Word documents and PDF files. Last seen in 2010, PinchDuke largely targeted user credentials for services like Yahoo, Google Talk, and Mail.ru.

2009

The first known campaigns targeting the West began in 2009 when the group targeted Georgia's Ministry of Defense, the Ministries of foreign affairs of Turkey and Uganda, the North Atlantic Treaty Organization (NATO), and an unnamed U.S. foreign policy think tank.

2010

In the spring of 2010, APT29 began targeting member countries of the Commonwealth of States with a new information stealing malware toolset called "CosmicDuke." Upon infecting a device, the malware has the potential to steal the user's login credentials from browsers and software programs.

2011

Prior to 2011, APT29 expanded their infrastructure through compromising websites and renting servers to use for Command and Control. During 2011, the group began to register domains with the name "John Kasai of Klagenfurt, Austria." With new infrastructure also came "CozyDuke" and "MiniDuke." MiniDuke was a backdoor for receiving and executing commands on an infected machine. CozyDuke was a malware platform with different modules that could be used for various objectives.

2012

APT29 did not add new tactics or malware in 2012.

2013

In February of 2013, FireEye announced the discovery of an Adobe Reader zero-day exploit which APT29 exploited to drop a previously unknown, advanced piece of malware dubbed "ItaDuke" by researchers. Several additional attacks used the same exploit (CVE- 2013-0640) and were dubbed MiniDuke by Kaspersky Lab researchers.

2014

In February 2014, Kaspersky Lab researchers found that CosmicDuke had resurfaced. This version was able to spoof the names and icons of recognizable applications and gain persistence by creating a task through Windows Task Scheduler. This window allowed the Miniduke backdoor downloader component to update and increase the malware's stealth capabilities.

Later in 2014, APT29 created OnionDuke, which contained modules for DDos attacks, ID theft, and password theft. OnionDuke was used to create a botnet that contained approximately 1400 compromised machines. The exact use of the botnet remains unclear.

2015

In July of 2015, FireEye researchers revealed APT29 was using a new custom malware called "Hammertoss 4." The malware manipulates legitimate services (e.g. Twitter and Github) for command and control communication.

2016

In June 2016, Cozy Bear was implicated alongside Fancy Bear in the Democratic National Committee cyber attacks. CrowdStrike concluded that APT29 had likely gained access to the DNC network through a spear phishing email during the summer of 2015. The spear phishing emails launched during this timeframe were mainly used to redirect victims to a malicious website that led to a dropper hosted on the webpage. The dropper, once activated, would download one of multiple Remote Access Trojans (RATs).

2017

In March 2017, FireEye Mandiant researchers reported that APT29 was employing a new technique called “domain fronting.” Domain fronting enabled APT29 to bypass censorship by making traffic look like it was generated by a valid domain.

2018

In 2018, FireEye devices detected intrusion attempts against multiple industries. One of which used a phishing email, disguised as legitimate correspondence from the U.S. Department of State with links to zip files containing malicious Windows shortcuts that delivered the Cobalt Strike Beacon.

2019

2019 led to the discovery of Cozy Bear’s three new malware families—PolyglotDuke, RegDuke and FatDuke. Compromises using these packages are collectively referred to as Operation Ghost.

2020

According to a joint advisory from the US’s National Security Agency and the UK’s National Cyber Security Center, and Canada’s Communications Security, APT29 tried to steal research on COVID-19 vaccines by using malware and spear phishing. Russian government hackers, known as APT29, breached the Treasury and Commerce departments, along with other U.S. government agencies, as part of a global espionage campaign that stretches back months.

Cozy Bear Malware

CloudDuke

The CloudDuke malware is composed of a downloader, a loader, and two backdoors, which download and execute from either web address or from a Microsoft OneDrive account.

GeminiDuke

The malware consisted of a loader, an information stealer, and numerous persistence components.

CosmicDuke

Discovered in 2014, CosmicDuke uses the old style Miniduke implants from 2013 that are still around and are being used in active campaigns that target governments and other entities.

HAMMERTOSS

The Hammertoss malware strain uses network traffic noise from sources including Twitter and GitHub to spy upon corporate victim machines for longer.

CozyCar

It is a modular malware platform, and its backdoor component can be instructed to download and execute a variety of modules with different functionality.

MiniDuke

Miniduke/CosmicDuke is capable of starting via Windows Task Scheduler, via a customized service binary that spawns a new process set in the special registry key, or is launched when the user is away and the screensaver is activated.

OnionDuke

OnionDuke is a malware family that was distributed via the Tor network.

POSHYSPY

Mandiant observed APT29 using a stealthy backdoor that FireEye called POSHSPY. POSHSPY leverages PowerShell and Windows Management Instrumentation (WMI) to deploy secondary backdoors for use, in case they lose access to primary backdoors.

SeaDuke

The Seaduke trojan is a low-profile information-stealer, used against few high-value targets and deployed against government-level targets in the United States and Europe.

WellMail

WellMail is a lightweight tool designed to run commands or scripts with the results being sent to a hardcoded Command and Control (C2) server.

PinchDuke

The PinchDuke campaign is believed to be the first campaign of the Duke malware family, delivered via phishing emails that contained spoofed news articles from official news sources. The malware consists of multiple loaders and an information stealer trojan.

PowerDuke

PowerDuke is a backdoor that was primarily delivered through Microsoft Word or Excel attachments containing malicious macros.

SoreFang

This malware is a first stage downloader that uses HTTP to exfiltrate victim information and download second stage malware.

WellMess

WellMess is a lightweight malware designed to execute arbitrary shell commands, upload and download files.

PolyglotDuke

PolyglotDuke is a downloader that has been used by APT29 since at least 2013. PolyglotDuke has been used to drop MiniDuke.

RegDuke

RegDuke is a first-stage implant that the hackers employ when losing control of other implants on the same machine. The malware was designed to remain undetected for as long as possible, to ensure the attackers never lose access to the compromised system.

SUNBURST

A trojanized version of a digitally signed SolarWinds Orion plugin called SolarWinds.Orion.Core. BusinessLayer.dll. The plugin contains a backdoor that communicates via HTTP to third party servers.

Closing Notes

APT29 is largely focused on long-term espionage campaigns with communication obfuscation to disguise their stealth attacks. Yet even sophisticated hackers can leave behind footprints in the Domain Name System (DNS), the infrastructure of the Internet. The DNS is a part of all cyber activities, good and bad. Historical passive DNS data enables threat hunters, incident responders and other security professionals to uncover these footprints as well as map an adversary's malicious infrastructure using a single IP address or domain name. Farsight's passive DNS database (DNSDB) provides a rich history of DNS records dating back to 2010.

Summary

Names

APT29, Dukes, Group 100, Cozy Duke, EuroAPT, Cozy Bear, CozyCar, Cozer, Office Monkeys/TEMP. Monkeys, Minidionis, SeaDuke, Hammer Toss, Fritillary, Yttrium, IRON HEMLOCK, Operation Ghost.

Toolsets and Malware

Hammertoss, OnionDuke, CosmicDuke, MiniDuke, CozyDuke, SeaDuke, SeaDaddy implant developed in Python and compiled with py2exe, AdobeARM, ATI-Agent, MiniDionis, Grizzly Steppe, Vernaldrop, Tadpole, Spikerush, POSHSPY, PolyglotDuke, RegDuke, FatDuke.

Targets

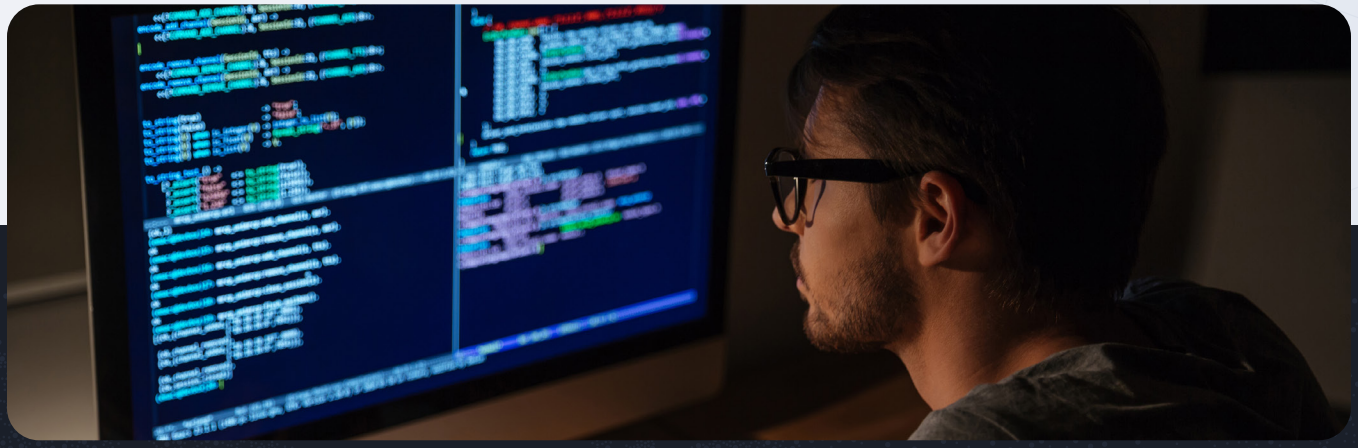
This threat actor targets government ministries and agencies in Europe, the US, Central Asia, East Africa, and the Middle East. They have also been associated with the DNC hacks ahead of the 2016 presidential election DNC attacks. They remain active.

Modus Operandi

Phishing emails

REFERENCE

- https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/
- https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
- https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf
- http://www.volexity.com/blog/
- https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf
- https://www2.fireeye.com/rs/848-DID-242/images/RPT-M-Trends-2017.pdf
- https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html
- https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html
- https://securelist.com/the-cozyduke-apt/69731/
- https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/



About DomainTools

DomainTools is the global leader for Internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape.

View our Farsight DNSDB page

DomainTools

FARSIGHT SECURITY
A DOMAINTOOLS COMPANY