informa

InformationWeek IT NETWORK | Dark Reading | Network Computing | About Us | Advertise | Register | Login to your account | Welcome Guest

DARKReading | SIGN UP FOR OUR NEWSLETTERS | Search Dark Reading

Authors | Slideshows | Video | Tech Library | University | Radio | Calendar | Black Hat News | Follow DR:

THE EDGE | ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | OPERATIONS | PERIMETER | RISK | THREAT INTELLIGENCE | VULNS / THREATS

VULNERABILITIES / THREATS

7/25/2017
07:00 PM

Jai Vijayan
News

Connect Directly

0 COMMENTS
COMMENT NOW

Login
50% 50%

Like
Tweet
Share

Iranian Cyber Espionage Group CopyKittens Successful, But Not Skilled

Despite being only moderately skilled, CopyKittens has exfiltrated large volumes of data since at least 2013.

It doesn't always take a highly skilled adversary to create major problems for organizations. Sometimes, unsophisticated but persistent threat actors can be just as effective at it.

One example is CopyKittens, a cyber espionage group with links to Iran that has been operating since at least 2013. The group, profiled in a report this week from Israel-based ClearSky Cyber Security and Trend Micro, so far has displayed little of the sophistication associated with many modern state-sponsored cyber espionage operations.

Yet, it has successfully managed to exfiltrate large volumes of data from targeted military and government organizations, academic institutions, municipal authorities and IT companies in Israel, Turkey, Saudi Arabia, Jordan, and the United States.

In the years it has been around, the group has used dozens of domains, many of them impersonating companies such as Microsoft, Google, Amazon, Facebook, and Oracle, for malware delivery, hosting malicious sites, and for command-and-control.

Despite its apparently limited resources, the group has also managed to breach several online news media outlets and general websites, which were then used in watering hole attacks.

"They are in the lower bar of cyber espionage groups," says Eyal Sela, head of threat intelligence at ClearSky. "They don't use 0-days and their self-developed tools are inferior in many aspects to those of others."

The group's tactics, techniques and procedures (TTPs) in general have been unremarkable and have included common approaches such as malicious email attachments, phishing, web application attacks, and, starting only late 2016, a few watering hole exploits.

Their continued success highlights how a persistent but relatively unadvanced threat actor can still succeed and reach their objectives, Sela says. "Organizations in sectors and countries of interest to Iran are at risk of being targeted," and should make it a point to understand the group's TTPs he cautions.

For example, CopyKittens has a tendency to try and breach an organization's network via weaknesses in the IT supply chain. It also has a tendency to do a lot of DNS-based data exfiltration and command-and-control so organizations that believe they could be targets should monitor their DNS infrastructure. Similarly, social media channels—such as fake Facebook profiles—have often been used to get close to and breach target organizations, Sela said.

This week's report on CopyKittens marks the third time that ClearSky has published an analysis of the threat group. The new report includes some fresh details on the group's activities, details on newly developed malware and a list of tens of new domains that are currently up and running and being used by CopyKittens for malware delivery and attacks.

Among the newly developed malware samples described in the Clear Sky and Trend Micro report this week is a .NET backdoor that provides attackers with a way to download and execute malware on a target system, and a tool that enables lateral movement in a compromised network using stolen credentials. AV tools in VirusTotal did not detect several of the new tools developed by the group.

Many of the tools that the group has used to exploit networks have legitimate purposes. For example, CopyKittens often has used a trial version of a commercial software tool called Cobalt Strike to search for and penetrate vulnerabilities in target networks. Other similar tools that it has used include Metasploit, Mimikatz, and software like Havij for detecting vulnerable web servers.

"It seems that their objective is to gather as much information and data from target organizations as possible," Sela says. "They indiscriminately exfiltrate large amounts of documents, spreadsheets, files containing personal data, configuration files, and, databases."

The sheer scope and duration of the campaign suggests that CopyKittens is a nation-state sponsored group, he says. The fact that the threat actor does not appear motivated by financial gain, and its multiple ties to Iran and Iranian interests suggest strong nation-state support, he added.

Related content:

- Iranian Hackers Believed Behind Massive Attacks on Israeli Targets
- Iran Intensifies Its Cyberattack Activity
- Saudi Arabia Issues Alert On Shamoon 2
- 8 Hot Hacking Tools to Come out of Black Hat USA

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year ... View Full Bio

COMMENT | EMAIL THIS | PRINT | RSS

MORE INSIGHTS

Webcasts
- Building an Enterprise Strategy for Detection and Response (XDR)
- Cyber Attack Evasion Techniques

MORE WEBCASTS

White Papers
- 2020 IT Salary Survey Results Revealed
- NetFlow vs Packet Data

MORE WHITE PAPERS

Reports
- 2020 IT Salary Survey Results Revealed
- [Report] DevSecOps & Secure App Delivery: What's Working & What's Not

MORE REPORTS

COMMENTS

NEWEST FIRST | OLDEST FIRST | THREADED VIEW

Be the first to post a comment regarding this story.

HOT TOPICS | EDITORS' CHOICE

Many Ransomware Attacks Can be Stopped Before They Begin 2
Jai Vijayan, Contributing Writer, 3/17/2020

Why CSP Isn't Enough to Stop Magecart-Like Attacks 1
Hadar Blutrich, CTO & Co-founder, Source Defense, 3/11/2020

How the Rise of IoT Is Changing the CISO Role 1
Phil Neray, VP of IoT & Industrial Cybersecurity at CyberX, 3/11/2020

SUBSCRIBE TO NEWSLETTERS

WEBINARS

Building an Enterprise Strategy for Detection and Response (XDR)

The ROI Story: Identifying & Justifying Disruptive Technology

5 Steps to Integrate SAST into the DevSecOps Pipeline

WEBINAR ARCHIVES

WHITE PAPERS

- 2020 IT Salary Survey Results Revealed
- NetFlow vs Packet Data
- 2020 Trends to Watch: Cybersecurity
- Network Traffic Analysis Instrumentation Guide
- 5 Ways to Get Better Data for Incident Response and Threat Hunting

MORE WHITE PAPERS

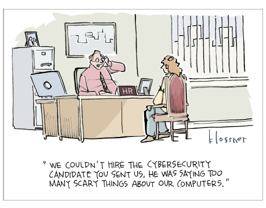
VIDEO

Ransomware Trains Its Sights on Cloud ...
6 COMMENTS

Qualys Launches Free App for IT Asset ...
1 COMMENTS

ALL VIDEOS

CARTOON



HR
Klossner
" WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US, HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."

Latest Comment: Unfortunately nobody wants to spend money on security. Usually they change their mind but often it is too late

CARTOON ARCHIVE

CURRENT ISSUE

Tech Digest
DARK Reading
AI
6 Emerging Cyber Threats Enterprises Face in 2020
Attackers using artificial intelligence and machine learning tools will give IT security pros new challenges to deal with this year and the years ahead.

6 Emerging Cyber Threats That Enterprises Face in 2020

This Tech Digest gives an in-depth look at six emerging cyber threats that enterprises could face in 2020. Download your copy today!

DOWNLOAD THIS ISSUE!

BACK ISSUES | MUST READS

FLASH POLL

Has the U.S. political climate caused you to make infosecurity-related changes to your disaster recovery/business continuity plans?

○ Yes

○ No

○ No but we are considering it

○ Still waiting for cybersecurity guidance from Trump admin EO

○ Don't know

○ Other (Please explain in the comments)

Submit

ALL POLLS

REPORTS

DARKReading REPORTS
How Enterprises Respond to the Incident Response Challenge
Data breaches and regulations have forced organizations to pay closer attention to the security incident response function. However, security leaders may be overestimating their ability to detect and respond to security incidents.
paloalto
CORTEX

State of Cybersecurity Incident Response

Data breaches and regulations have forced organizations to pay closer attention to the security incident response function. However, security leaders may be overestimating their ability to detect and respond to security incidents. Read this report to find out more.

DOWNLOAD NOW!

How Enterprises Are Developing and Maintaining Secure Applications — 0 COMMENTS

How Enterprises are Attacking the Cybersecurity Problem — 0 COMMENTS

How Data Breaches affect the Enterprise — 0 COMMENTS

MORE REPORTS

TWITTER FEED

BUG REPORT

ENTERPRISE VULNERABILITIES
From DHS/US-CERT's National Vulnerability Database

- **CVE-2020-3922**
  PUBLISHED: 2020-03-18
  LisoMail, by ArmorX, allows SQL Injections, attackers can access the database without authentication via a URL parameter manipulation.
- **CVE-2020-10659**
  PUBLISHED: 2020-03-18
  Entrust Entelligence Security Provider (ESP) before 10.0.60 on Windows mishandles errors during SSL Certificate Validation, leading to situations where (for example) a user continues to interact with a web site that has an invalid certificate chain.
- **CVE-2020-8468**
  PUBLISHED: 2020-03-18
  Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) agents are affected by a content validation escape vulnerability which could allow an attacker to manipulate certain agent client components. An attempted attack requires user authentication.
- **CVE-2020-8470**
  PUBLISHED: 2020-03-18
  Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow an attacker to delete any file on the server with SYSTEM level privileges. Authentication is not required to exploit this vulnerability.
- **CVE-2020-8598**
  PUBLISHED: 2020-03-18
  Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow a remote attacker to execute arbitrary code on affected installations with SYSTEM level privileges. Authentication is not required to exploit th...