Connecting Taidoor’s Dots: Earth Aughisky Over The Last 10 Years

Archived: 2026-04-05 18:06:28 UTC

open on a new tabDownload The Rise of Earth Aughisky: Tracking the Campaigns Taidoor Started

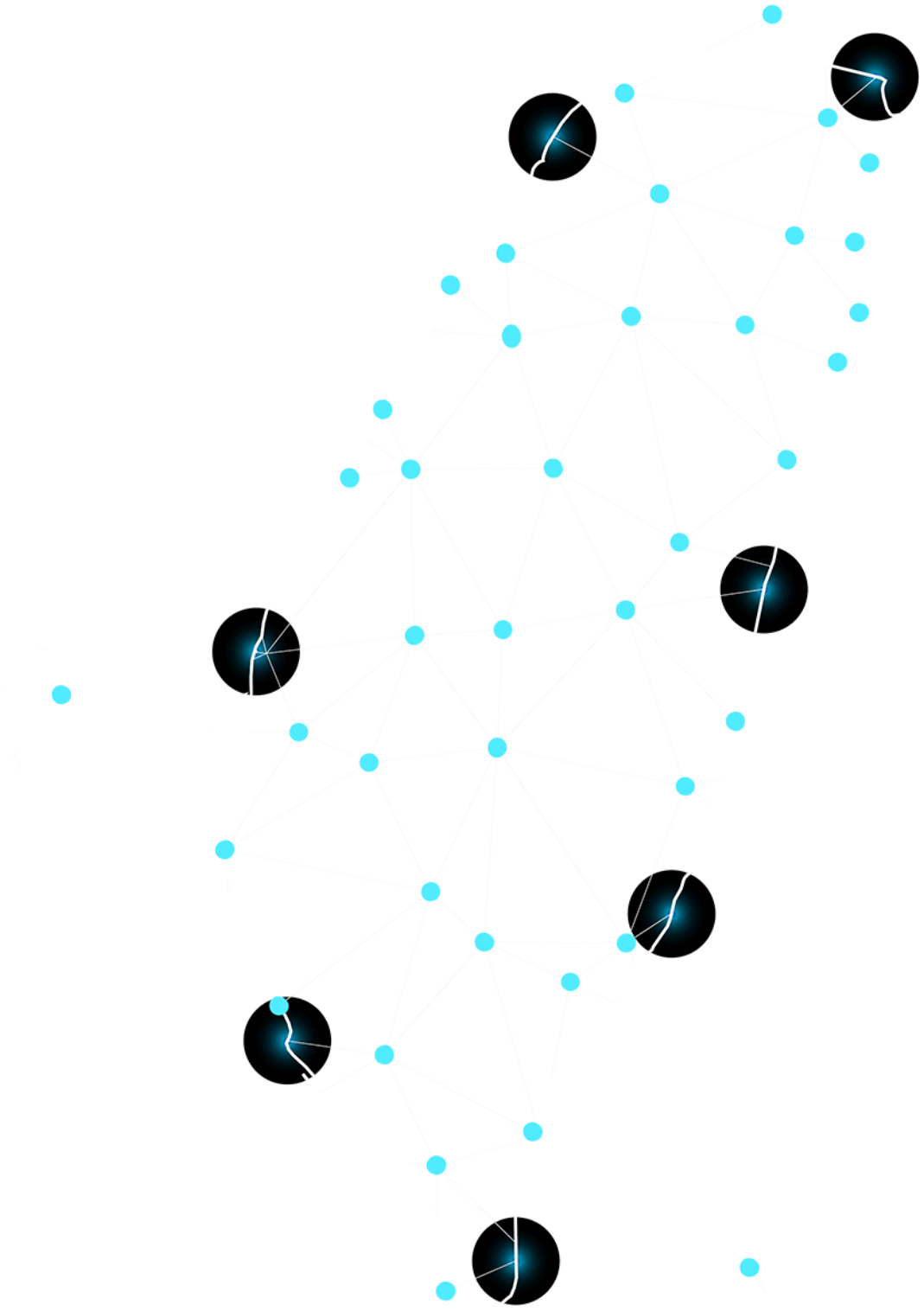
Trend Micro uses Earth Aughisky to refer to the APT group, while Taidoor is used to refer to one of the malware families deployed by the group for campaigns.

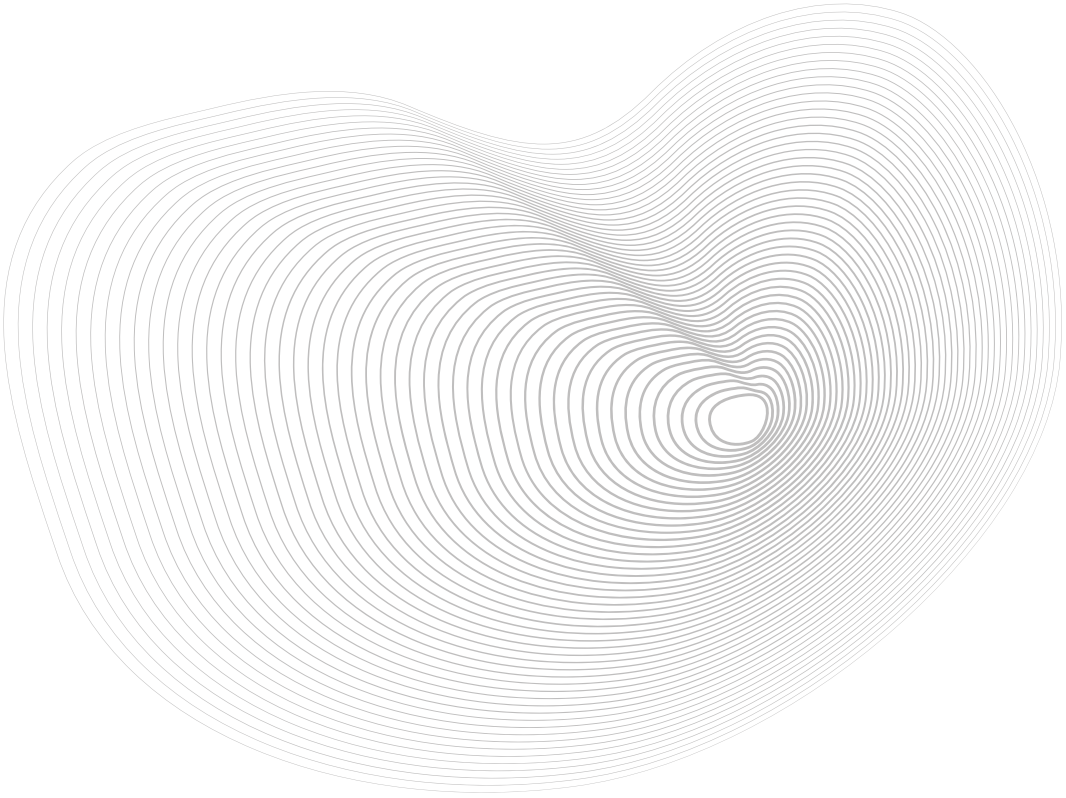
open on a new tabDownload The Rise of Earth Aughisky: Tracking the Campaigns Taidoor Started

Since its first documented activity in 2011, advanced persistent threat (APT) group Earth Aughisky's campaigns continued to plague organizations' operations and disrupt everyday activities. Trend Micro's monitoring of the group over the last decade yielded significant patterns for attribution, connections, and even changes. This cyberespionage group expends efforts at evading detection once inside targets' systems by abusing legitimate accounts, software, applications, and other potential weaknesses in the network design and infrastructure.

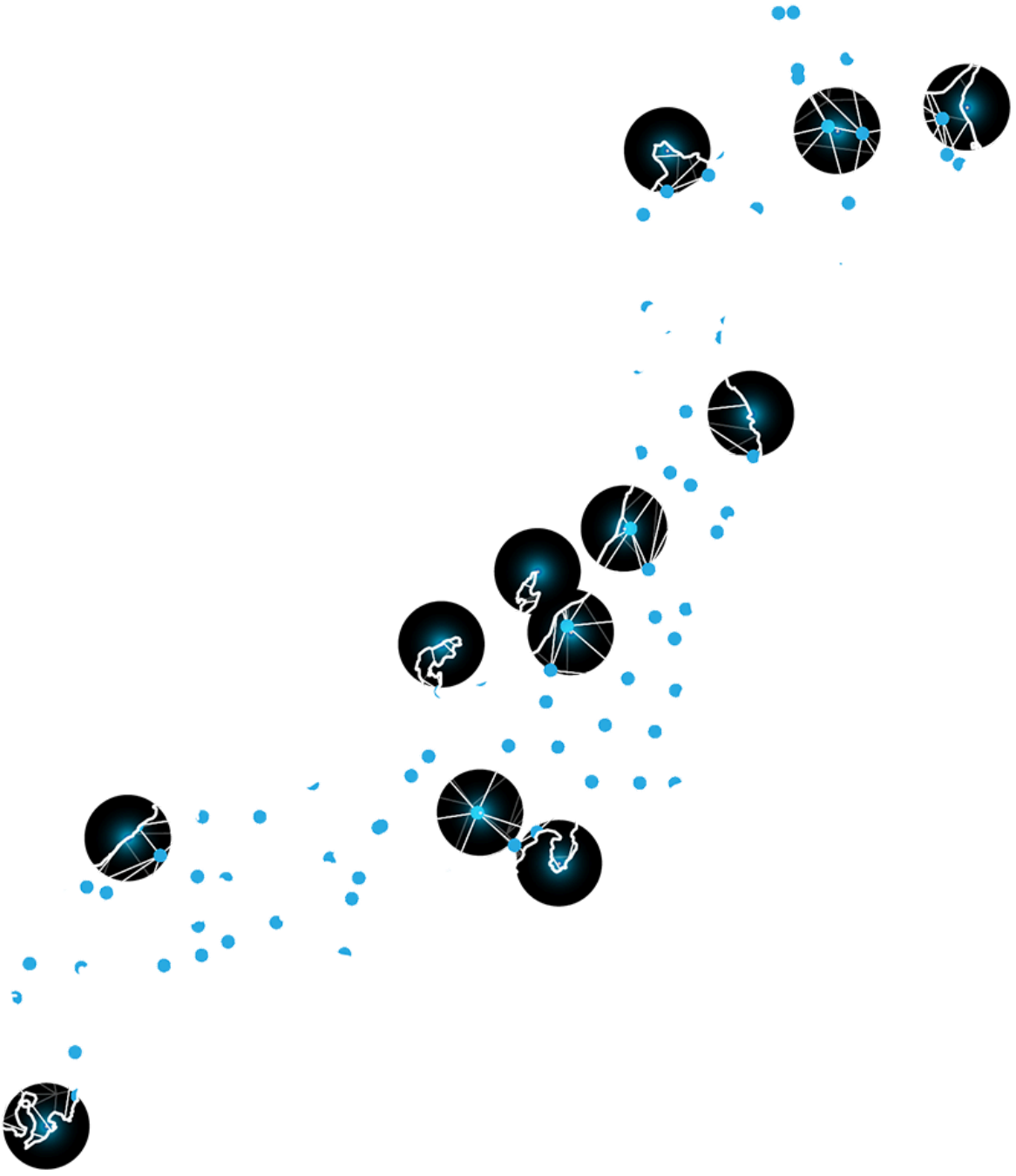
Tracking this APT group's history and continuous activities has allowed researchers and cybersecurity practitioners to learn its movements, technical developments, and potential relationships with other cybercriminal and cyberespionage groups.

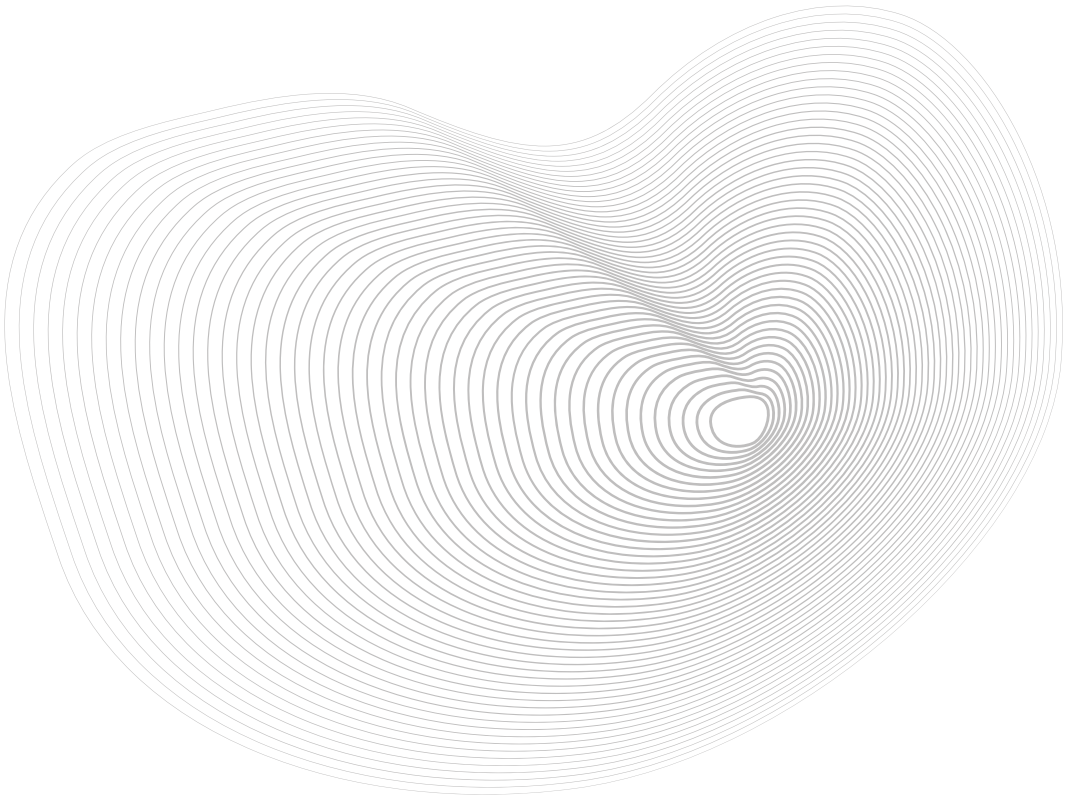
Targeting background





Observations of Earth Aughisky's campaign deployments were primarily found to be focused on organizations in Taiwan, consistently updating its arsenal to circumvent developments in security solutions. Over the last decade, our analyses have observed the malware families' and tools' increasing sophistication, until more recent changes in their routines indicated potential changes in the APT's organization.



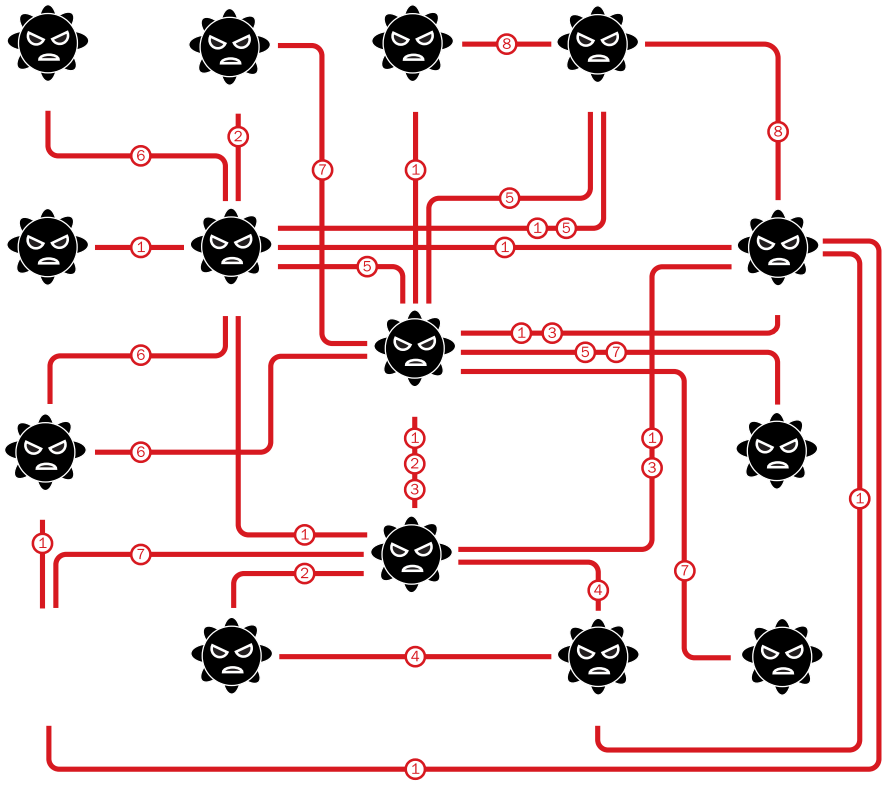


We observed that the cyberespionage group began expanding their targets to Japan towards the end of 2017, potentially suggestive of changes in the sponsor's objectives and real-world organizational structures. This is also evident in the other changes security analysts have tracked occurring in recent years, such as malware arsenal use and infrastructure.

Malware connections

In the research paper, "The Rise of Earth Aughisky: Tracking the Campaigns Taidoor Started,"open on a new tab researchers listed the analysis of all the malware families previously attributed to the group. These studies on the routines and tools documented from previous samples and incidents revealed similarities with a number of malware families and tools that have yet to be attributed to Earth Aughisky or seen being used by other cyberespionage groups.

Here is a summary of the malware families and tools attributed to Earth Aughisky, how each are connected, and brief technical and historical descriptions of each. Click on each of the malware families to find the year of disclosure and a brief description.



- IP/Domain/Passive DNS overlap
- Host on same repository
- Same function (logging/proxy)
- Payload and downloader
- Special string (marker/class name)
- Same incident
- Same loader/Dropper
- Same campaigns code/Password

- **Kuangdao (also known as KD)**
    - Year tracked: 2007
    - This malware's name was based on the .pdb string observed and matched in multiple backdoor configurations, and shared similarities with a number of Earth Aughisky's malware families.

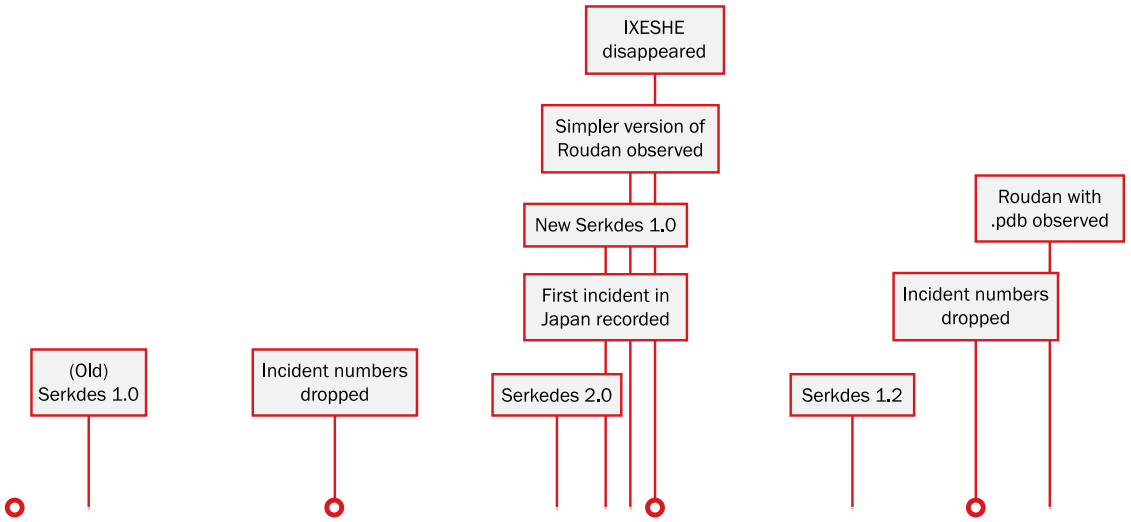
- **Specas**
    - Year tracked: 2008
    - Specas was previously identified as Roudan or Taleret; behavior analysis showed a difference from both malware families in functions.

- **GOORAT**
    - Year tracked: 2009
    - A backdoor preceding Taleret and no longer in use, samples of GOORAT were configured to retrieve data from Google groups or blogs.

- **TWTRAT**
    - Year first documented: 2010
    - An old backdoor used for a short period, TWTRAT abused direct messages in social media platform Twitter for C&C communication.
- **ASRWEC Downloader**
    - Year first documented: 2011
    - A downloader capable of searching for payloads — either Roudan or SiyBot, or both — in blogs and other repositories.
- **SiyBot**
    - Year first documented: 2011
    - A backdoor not yet documented and rarely observed in a few attack incidents, it abused legitimate applications such as Gubb or 30 Boxes for C&C communication.
- **Roudan**
    - Year first documented: 2011
    - The malware first attributed to Earth Aughisky using different callback traffic techniques.
- **K4RAT**
    - Year first documented: 2012
    - Active between 2012 to 2016, this backdoor contained basic functions for collecting system information from targets.
- **Comeon Downloader**
    - Year first documented: 2012
    - A downloader used to deliver Roudan malware from private servers and repositories.
- **Illitat Downloader**
    - Year first documented: 2012
    - This downloader collected system information and used the local environment to call back to the C&C server and downloads Roudan malware.
- **Taleret (also known as Dalgan)**
    - Year first documented: 2013
    - Marked to run with different implementations — XXXXX and Artemis — this malware abused public blogs and other repositories to locate the command and control (C&C) configurations.

- **GrubbyRAT**
    - Year first documented: 2014
    - This rarely deployed backdoor was observed from attacks seemingly categorized based on indicators on the targets such as value, criticality, sensitivity, economic stature, and/or industry, among others.
- **Buxzop/DropNetClient**
    - Year first documented: 2015
    - While DropNetClient has been previously documented, Buxzop is its updated version. This malware uploaded and stole victim information by abusing a DropBox API for C&C communication.
- **Taikite (also known as SVCMONDR)**
    - Year first documented: 2015
    - Taikite was first identified with a routine reportedly abusing CVE-2015-2545, but no other reports attribute this malware to Earth Aughisky.
- **Serkdes (also known as Yalink)**
    - Year first documented: 2018
    - This malware was documented to have several conflicting versions and samples, strongly indicative that this was used by more than one APT group. This backdoor was also identified in attacks on Japanese organizations.
- **LuckDLL**
    - Year first documented: 2021
    - LuckDLL is a relatively new backdoor, and some samples have been observed containing one of two program database strings in .pdb.

Updates and changes



The longevity of Earth Aughisky in the cyberespionage world allows cybersecurity researchers and analysts to follow patterns, and even notice subtle changes when they occur. For instance, the recent changes in activity frequency, overlaps in malware and tools attributed to other groups, and even the simplification in codes of known and established malware have attracted attention. These subtle series of deviations have prompted researchers to match real-world changes of known sponsors, take a closer look at other groups, and reference potential changes in motivations and structures.

Conclusion and insights

Over the years, the consistent monitoring of APT group Earth Aughisky enabled cybersecurity researchers to gain insights into the inner workings of other similar cyberespionage groups. The amount of data gathered using various analysis techniques show an overview of motivations, the maturity of their technical skills, and even the plausible real-world connections of incidents. Groups like Earth Aughisky have sufficient resources at their disposal that allow them the flexibility to match their arsenal for long-term implementations of cyberespionage, and organizations should consider this observed downtime from this group's attacks as a period for preparation and vigilance for when it becomes active again.

Read our full analysis and recommendations on APT group Earth Aughisky in our research "The Rise of Earth Aughisky: Tracking the Campaigns Taidoor Started."open on a new tab The full list of indicators of compromise (IOCs) can be downloaded here.open on a new tab

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.
