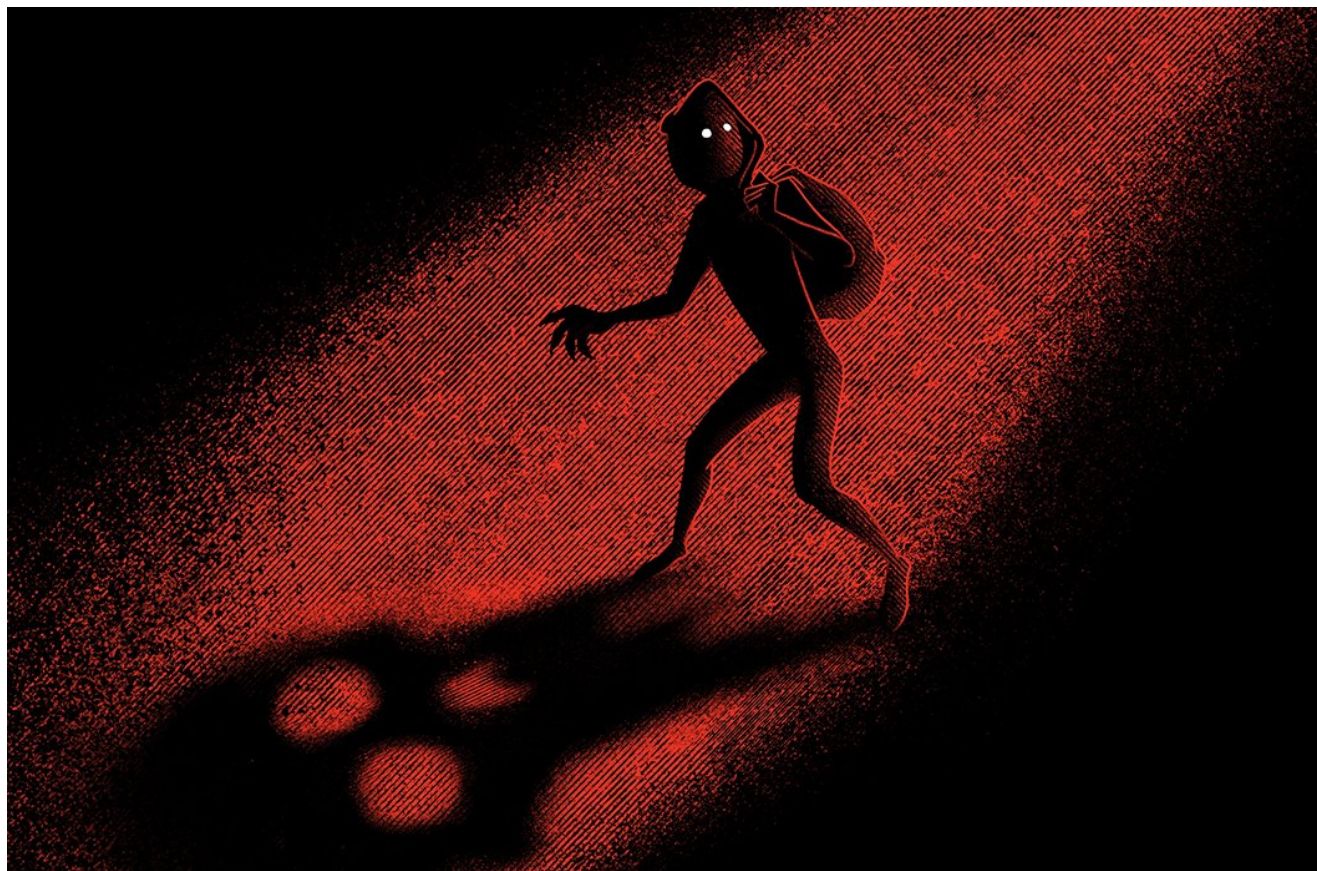


Shining a Light on DarkOxide

 crowdstrike.com/blog/darkoxide-technical-analysis/

Falcon OverWatch Team

September 15, 2021



Since September 2019, Falcon OverWatch™ has been tracking an as yet unattributed actor, conducting targeted operations against organizations within the Asia Pacific (APAC) semiconductor industry. CrowdStrike Intelligence tracks this activity cluster under the name DarkOxide.

CrowdStrike Intelligence has not yet determined the motivation of this activity cluster, but its tactics, techniques and procedures (TTPs) and target scope indicate it is more likely focused on the theft of sensitive information than on direct financial gain.

Telltale TTPs Reveal a Cluster of Activity

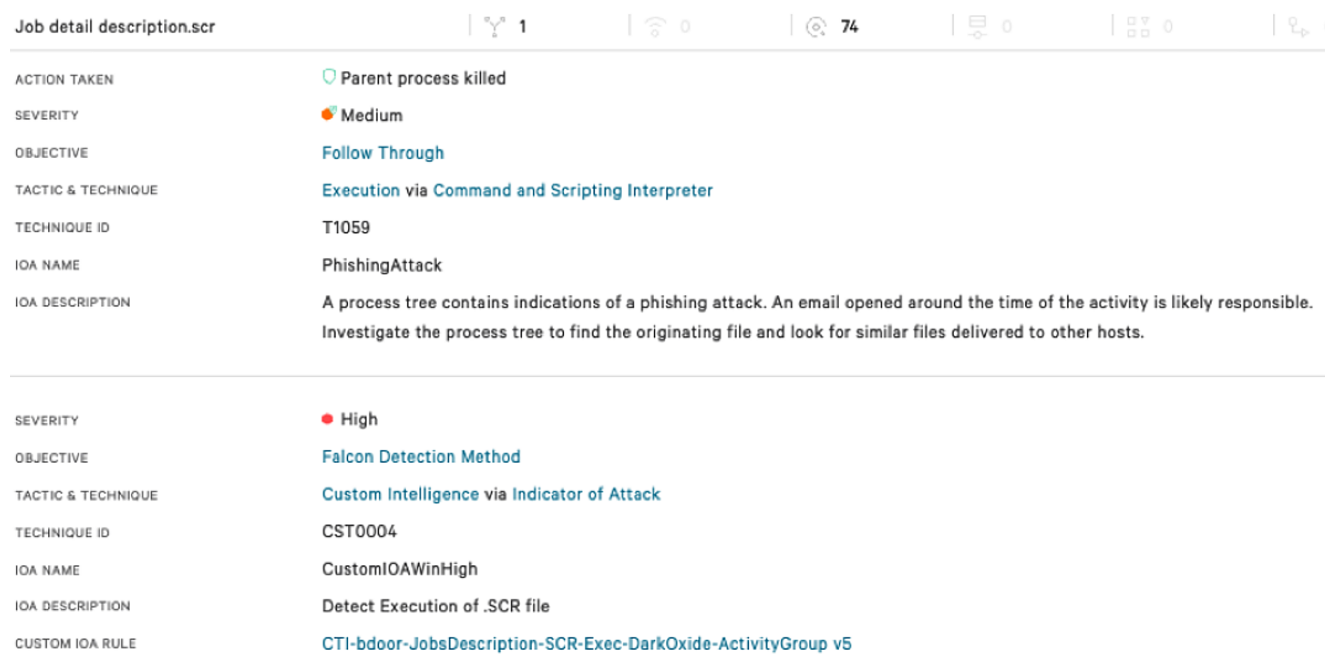
The DarkOxide cluster exhibits a very specific set of TTPs that have changed very little over the last two years.

Initially, the actor engages a target via a business-oriented social media platform under the guise of carrying out a recruitment drive (to read more about this technique, see <https://attack.mitre.org/techniques/T1566/003/>). The target is then encouraged to download a lure document purportedly relating to a job opening. In reality, this file is a malicious executable

with a double file extension. The executables in these lures have used non-standard executable file extensions such as .PIF (program information file) and .SCR (screensaver). As Windows, by default, hides the extension of known file types, these files initially appear to be legitimate document files when viewed in Windows File Explorer.

To date, the targets of the phishing attacks have included engineering staff with access to sensitive documents and source code, indicating that theft of intellectual property is the likely motivation for these operations.

The following screenshot shows the detection that appears in the CrowdStrike Falcon UI when a victim runs one of these malicious screensaver files. In this case, the customer had enabled preventions, allowing the pattern of activity to be recognized by the sensor and terminated before the actor could complete the installation of their remote access software.







(Click to enlarge)

When the payload is executed, it utilizes a number of scripting interfaces, including PowerShell and Visual Basic Script, to download a further malicious binary executable. This second executable, also with a .PIF or .SCR extension, in turn installs a copy of the legitimate remote access tool, Remote Utilities, with a preconfigured command-and-control (C2) address. In a small number of cases in addition to Remote Utilities, the actor also installed the Total Manager Pro file manager. It is likely that this was in order to conduct file system searches, or to package files for exfiltration.

Although the Remote Utilities binary, `rutserv.exe`, is a legitimate signed binary, its use is relatively rare across CrowdStrike's customer set.

As of at least March 2020, this TTP has been slightly modified, removing the first stage downloader and moving directly from the initial phishing attack to the installation of the Remote Utilities software.

The following table shows how these TTPs have been shared across a number of intrusions and how they map to the MITRE ATT&CK® framework.

	 Initial Access	 Execution	 Command & Control	 Persistence
	Phishing: Spearphishing via Service T1566.003	Command & Scripting Interpreter: PowerShell and Visual Basic T1059.001 & T1059.005	Remote Access Software T1219	Event Triggered Execution: Screensaver T1546.002
Semiconductor 1	X	X	X	X
Semiconductor 2	X		X	X
Semiconductor 3	X		X	X
Telecommunications	X	X	X	
Semiconductor 4	X	X	X	X

In June 2021, the cluster was observed deploying additional tooling to a host. Again these tools were commercial off-the-shelf software. The tooling observed included:

- Total Spy: a commercial spyware suite with capabilities including keylogging, screen capture, messaging capture and social network capture
- RDP Wrapper: an open source tool allowing RDP access to the host
- DWServe: an open source tool allowing the host to be remotely controlled from a web browser

In almost all cases, the cluster’s activity has been frustrated, either by preventions enabled by the customer, or by early notifications from Falcon OverWatch, allowing the affected systems to be contained before the actor could take further actions on objectives. In the single case where follow-up activity was observed, it consisted of modifications to the registry in order to allow further access to the host via Remote Desktop Protocol. (To read more about these techniques see: <https://attack.mitre.org/techniques/T1112/> and <https://attack.mitre.org/techniques/T1133/>.)

Since CrowdStrike began tracking DarkOxide, the activity cluster has continued to conduct operations against a number of semiconductor companies, almost exclusively located within the South Asia region.

Your Best Defense Against DarkOxide

Over the past two years, Falcon OverWatch, alongside CrowdStrike Intelligence, has been tracking an activity cluster, DarkOxide, actively targeting the semiconductor industry. Although the actor’s TTPs have remained largely consistent, they have demonstrated the capacity to

adapt and improve their processes, having recently streamlined their activity by removing the need for a first-stage downloader in their intrusion process.

Defenders in the semiconductor industry should be particularly alert to this activity, which drives home the need to enlist end users as the first line of defense. The actor is actively targeting employees via social media to gain initial access. Well-trained staff can be an asset in combating the continued threat of phishing and related social engineering techniques.

As noted above, the Falcon platform can identify and prevent actors' use of malicious files with double extensions, but it is crucial the sensor is rolled out across the environment with appropriate prevention settings turned on. Defenders can slow down malicious activity by employing strict user account management based on the principle of least privilege.

Finally, but most crucially, this activity shows the lengths to which threat actors go in their attempt to evade automated detections. Whether by gaining access through phishing activities, or by using legitimate tooling to achieve actions on objectives, threat actors are always looking for new ways to pierce an organization's defenses. A managed threat hunting service, like Falcon OverWatch, provides the continuous monitoring that is required to identify and disrupt malicious activity before the damage is done.

Indicators of Compromise

First Stage Payload

SHA256 Hash	Lure Filename
48c19ad7436f3d311e9e63327801d0a2d6d25c0d7c7bbc3d2c6a32afb95a0187	Final.exe
9d34f653edf948d9f46522081ff00ddd2f4b62b18d138c49e3b281ca953aeb1	Resume pdf.pif
1fcb6b54b17a6c3df0047a48280b4dcab8b2f2cad2ef4b8c802b05119cedce42	Talent Recruitment Web meeting system.pif
6d1480cd5b10739af130850f9d9bfa7ebe50024c5db68dd231bc7e4bd560ffa6	msi6.9.pif
9d68049510581ff4827fd72510c59d685ce54609b07733be17492bf2403442b4	Job description sr.scr
b414dca98e117d3755903ff27ffc07880f1fe2bfabfb49f6956cf82c06f4eab1	Job description sr.scr

8045f3e00e52c663ab942f39ec779ffc7ac90197ece8e574e5a70c422aa32b36	Job detail description.scr
49fbf9884299fbc6b09e640449fdc834f82a752908d381a68e2057a9861e3618	Job description.scr
186a7abdfcc2df113148650eb1673620a11bb8bfcf3c53f8a1c7429703cda715	Job detail description.scr
45e6653af40fb838eae0657a34905d5ba36052bd41819873d2afc240874b14b6	Qualcomm Job description India.scr
041398a0d34794df5b8d22683f5be7991647416f6243c7bc0441abd7c71c7c27	Qualcomm Job details.scr

Second Stage Payload

SHA256 Hash	Filename
9d34f653edf948d9f46522081ff00ddd2f4b62b18d138c49e3b281ca953aeb1	one.pif

Legitimate Binaries Observed

SHA256 Hash	Filename
5ada6d1fd62bb1740ea80a30788e55988758acc2b835e6835d6524af1e7afcbd	rutserv.exe
C295bd2653d6d8752ff5805b4114eee8e4370a0f16e922d81aecc5f49fa8c9c9	rfusclient.exe
966ef76fe3476d530b1b97a6f40947ed14ada378f13e44ecfe774edc998cd0b0	srvinst.exe
798af20db39280f90a1d35f2ac2c1d62124d1f5218a2a0fa29d87a13340bd3e4	rdpwrap.dll
07935229c213d1735655cc8453daa29718da2656546e05d5b3990cb49c248b98	RDPWInst.exe
43fbae4f6637c8eaa955db7e394eebd39cd261f91f36a5bc646303f123e68f13	tsmon.exe
39235102a3aeeb88678cad8d841292fc17ec3b0551cf57d755fdd523985567e8	tsmon4.exe
1ad4b06e282e3c3f22c6d194dabdc272215154f004c57b93b3882c161efc5279	tsmon5.exe
4515d7ee0d5e2e2e236499d35a154b427f07124e9edd379b6e9d62af2ae88c4d	tsmon6.exe

Hard-Coded Command and Control for Remote Utilities

- 54.149.69[.]226
- 54.188.107[.]146
- 60.254.95[.]183

- 34.221.96[.]116

Additional Resources

- *Download the newly released Falcon OverWatch annual report, [2021 Threat Hunting Report: Insights From the Falcon OverWatch Team](#).*
- *Find out more about adversaries that CrowdStrike Intelligence tracks in the [CrowdStrike Adversary Universe](#).*
- *Learn about the powerful, cloud-native [CrowdStrike Falcon® platform](#).*
- *[Get a full-featured free trial of CrowdStrike Falcon Prevent™](#) and see for yourself how true next-gen AV performs against today's most sophisticated threats.*