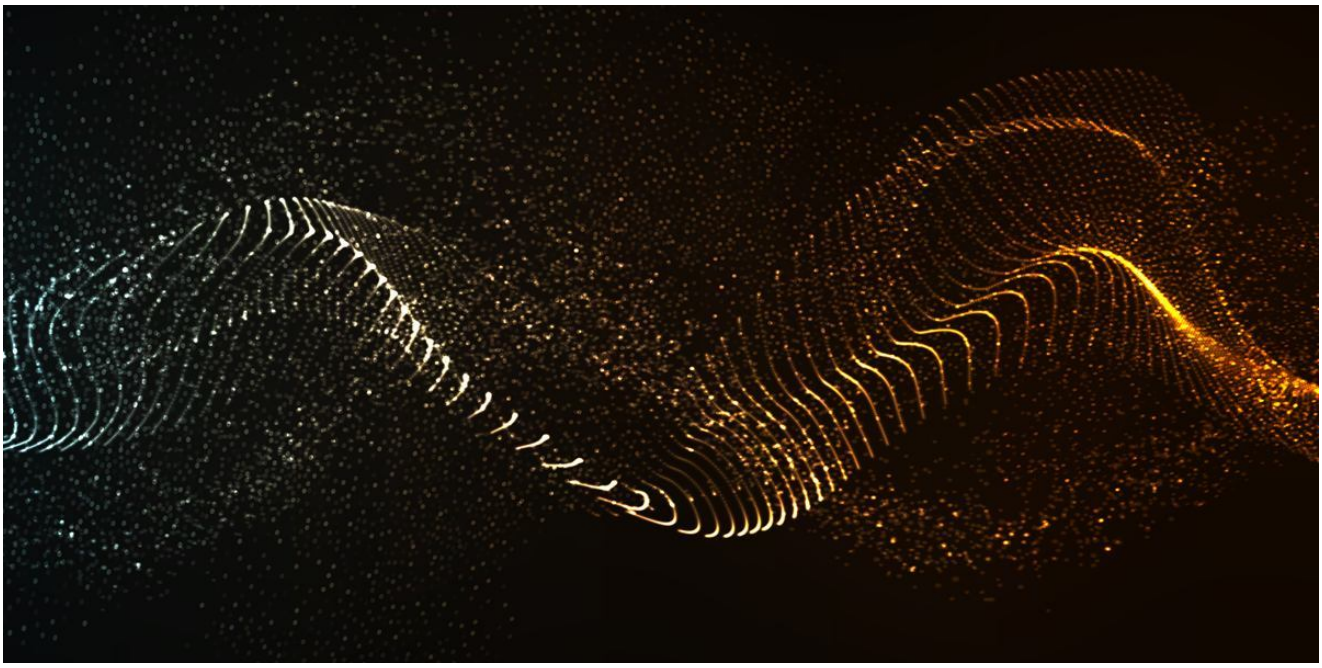
The resurgence of the Ursnif banking trojan

darktrace.com/en/blog/the-resurgence-of-the-ursnif-banking-trojan/



Max Heinemeyer, Director of Threat Hunting | Thursday July 23, 2020

Earlier this month, Darktrace's Cyber AI detected the Ursnif banking trojan, described as May's most wanted malware, making a resurgence across its customers' networks. This blog follows the malicious activity in one financial services company in the US, detailing how and why Darktrace Antigena stepped in and autonomously stopped the attack in real time.

Banking trojans continue to present a credible and persistent threat to organizations of all sizes across the globe. This attack was delivered via phishing email, which initiated a download of an executable file masquerading as a .cab extension.

This specific banking trojan is particularly sophisticated, with multiple new command and control (C2) domains registered – identifiable because several distinct Domain Generation Algorithms (DGA) were observed across different networks – the majority of which were only registered the day prior to the campaign.

Figure 1: A timeline of the attack

Phishing email catches organizations unaware

The malware itself was delivered via phishing email. The attack was not recognized by antivirus solutions at the time of delivery, slipping through the organization's perimeter solutions and landing in employees' inboxes. Unknowingly, an employee opened a disguised attachment containing macros, downloading an executable file masquerading as a .cab extension.

Interestingly, the malware also used new User Agents imitating Zoom and Webex, a clear attempt to blend in with assumed network traffic. After the malware was downloaded, several devices were observed making connections using these Zoom or Webex User Agents to non-Zoom and non-Webex domains, another attempt to blend in.


Figure 2: Darktrace's Breach Event Log shows a number of models were triggered


Figure 3: Darktrace's Device Event Log showing the device was connected to Outlook at the time of the executable file download

After the downloads, Darktrace's AI observed beaconing to rare DGA domains. The majority of these domains were Russian and registered within the previous 24 hours.


Figure 4: A screenshot taken from one of the C2 domains observed, tobmojiol2adf[.]com, which appears to host a login page


Figure 5: The External Sites Summary of one of the C2 domains observed, tobmojiol2adf[.]com, which was identified as 100% rare for the network at the time of the model breach.

This attack managed to evade the rest of the organization's security stack since the domains observed were recently registered and the majority of the file hashes and IoCs had not yet been flagged by OSINT tools, thus bypassing all signature-based detections. The initial file downloads also purported to be .cab files, but Darktrace's AI identified that these were in fact executable files.

Multiple Darktrace detections, including the 'Masqueraded File Transfer' model and the 'Initial Breach Chain Compromise' model, alerted the security team to this activity. At the same time, the models triggered Darktrace's Cyber AI Analyst to launch an automated investigation into the security incident, which surfaced additional vital information and dramatically reduced time to triage.


Figure 6: The Cyber AI Analyst output showing the subsequent C2 connections made by the device after the executable file download

Figure 7: Model breaches from the affected device, showing the malicious file download and subsequent command and control beaconing activity


Figure 8: Model Breach Event Log, showing Antigena's response after the masqueraded file download and a new outbound connection

The case for Autonomous Response

The Ursnif banking trojan presents a particularly lethal threat: silent, stealthy, and capable of stealing vital financial information, email credentials, and other sensitive data at machine speeds. The rise of advanced malware like this demonstrates the need for security technology that can stay ahead of attackers. For this organization, the malware download and subsequent command and control activity could have represented the start of a costly attack.

Luckily the organization had Antigena Network installed in active mode. The C2 communications from infected devices were blocked seconds after the initial connection, preventing further C2 activity and the download of any additional malware. Using information surfaced by the Cyber AI Analyst, the security team could catch up and the threat was quickly contained.

This attack highlights the continuously evolving approaches used by malicious actors to evade detection. In the same week as the events explained above, Darktrace identified the Urnsnif malware in numerous other customers in the US and Italy, across multiple industries. Attackers are targeting businesses indiscriminately and are not slowing down.

Thanks to Darktrace analysts Grace Carballo and Hiromi Watanabe for their insights on the above threat find.

To learn how cyber-criminals are using AI to augment their attacks, download the White Paper: The Battle of the Algorithms

Technical details

IoCs:

IoC	Comment
tobmojiol2adf[.]com	C2 domain, registered July 9
qumogtromb2a[.]com	Not yet registered
amehota2gfgh[.]com	C2 domain, registered July 8
gofast22gfor[.]com	C2 domain, registered July 8

xquptbabzxhxw[.]com	Not yet registered
e9bja[.]com	Masqueraded file download source
9ygw2[.]com	Masqueraded file download source
n2f79[.]com	Masqueraded file download source
ioyyf[.]com	Masqueraded file download source
hq3ll[.]com	Masqueraded file download source
hxxp://9ygw2[.]com/iz5/yaca.php?l=kpt1.cab	File path
hxxp://e9bja[.]com/iz5/yaca.php?l=kpt4.cab	File path
hxxp://n2f79[.]com/iz5/yaca.php?l=kpt1.cab	File path
hxxp://ioyyf[.]com/iz5/yaca.php?l=kpt4.cab	File path
hxxp://hq3ll[.]com/iz5/yaca.php?l=kpt12.cab	File path

MD5 hashes

- fa6fc057b3c1bb1e84cc37dbd14e7c10
- 37c28815f462115ff1439e251324ed5b
- 40f69d093a720c338963bebb3e274593
- 5602508f262b92f25dc36c4266f410b4
- 619e5f5d56de5dfbe7b76bba924fd631
- 30ea60c337c5667be79539f26b613449
- 688380643b0d70a0191b7fbbea6fb313
- 719f36d41379574569248e599767937f
- 7a7ba75af1210e707c495990e678f83e
- 7c4207591c6d07ce1c611a8bc4b61898
- 8eec0a8518e87d7248d2882c6f05a551
- 94915a540ce01fabec9ba1e7913837ea
- 94e6d6c3cef950ed75b82428475681c7
- bac0246599a070c8078a966d11f7089d
- dc17489e558d0f07b016636bc0ab0dbe
- dff18317acadc40e68f76d3b33ea4304
- cee72b840f4e79ed5ffde7adc680a7cd

SHA1 hashes

- 42dd5e8ad3f0d4de95eaa46eef606e24f3d253f0
- 97d2158a44b0eaa2465f3062413427e33cc2ac50
- 435c5ae175b40e5d64907bdb212290af607232eb

- 4b9845e5e7475156efa468a4e58c3c72cf0d4e7e
- a0494bf812cf1a5b075109fea1adc0d8d1f236f9
- 297b1b5137249a74322330e80d478e68e70add0d
- 46a9c4679169d46563cdebae1d38e4a14ed255c9
- 4f4f65acf3a35da9b8da460cf7910cd883fe2e46
- 60aee8045e0eb357b88db19775c0892f6bd388f1
- 7d92dad4971d3c2abfc368a8f47049032ef4d8a9
- 9631216035a58d1c3d4404607bd85bf0c80ccfe8
- aab6a948d500de30b6b75a928f43891f5daaa2a8
- c31dcf7bc391780ecf1403d504af5e844821e9a4
- c41a9a7f416569a7f412d1a82a78f7977395ce2a
- c7323a5596be025c693535fbb87b84beeacc7733
- d64a6c135d7eac881db280c4cb04443b7d2e2a0b
- 331ede8915e42d273722802a20e8bb9a448b39c5

Darktrace model breaches

- Anomalous File/Masqueraded File Transfer
- Compromise/ Sustained TCP Beaconing Activity to Rare Endpoint
- Compromise/ HTTP Beaconing to Rare Destination
- Compromise/ Slow Beaconing Activity to External rare
- Compromise/ Beaconing Activity to External Rare
- Device/ Initial Breach Chain Compromise

Max Heinemeyer

Max is a cyber security expert with over a decade of experience in the field, specializing in a wide range of areas such as Penetration Testing, Red-Teaming, SIEM and SOC consulting and hunting Advanced Persistent Threat (APT) groups. At Darktrace, Max oversees global threat hunting efforts, working with strategic customers to investigate and respond to cyber-threats. He works closely with the R&D team at Darktrace's Cambridge UK headquarters, leading research into new AI innovations and their various defensive and offensive applications. Max's insights are regularly featured in international media outlets such as the BBC, Forbes and WIRED. When living in Germany, he was an active member of the Chaos Computer Club. Max holds an MSc from the University of Duisburg-Essen and a BSc from the Cooperative State University Stuttgart in International Business Information Systems.