How a Fake Podcast Invite Delivers BlackSmith Malware | Proofpoint US

Published: 2024-08-15 · Archived: 2026-04-05 13:00:17 UTC

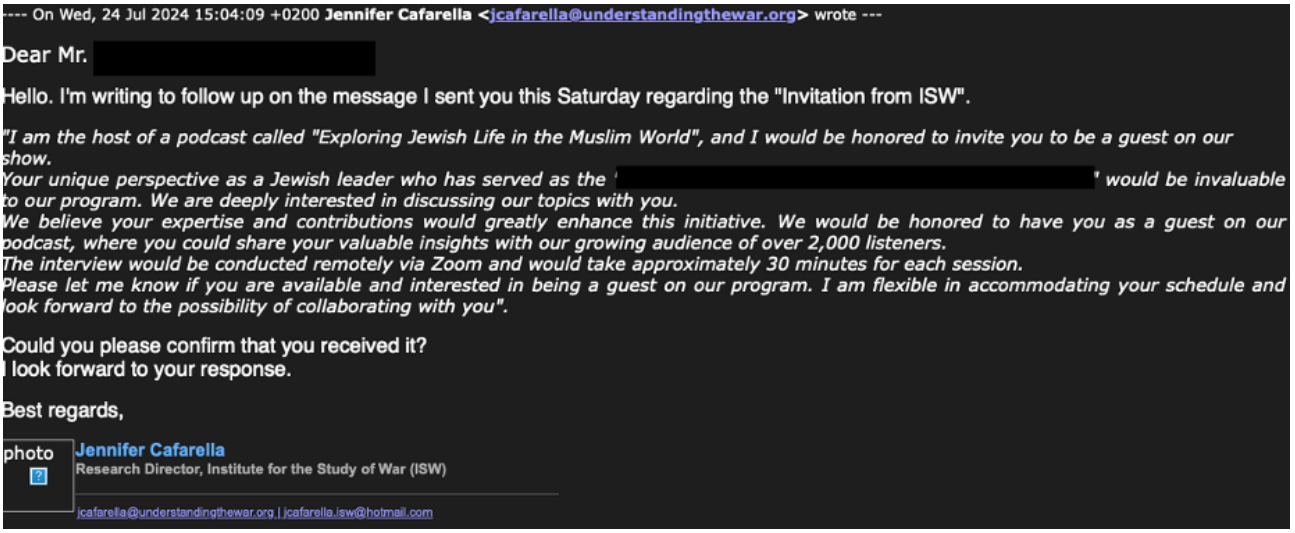
August 20, 2024 Joshua Miller, Georgi Mladenov, Andrew Northern, Greg Lesnewich and the Proofpoint Threat Research Team

Key findings

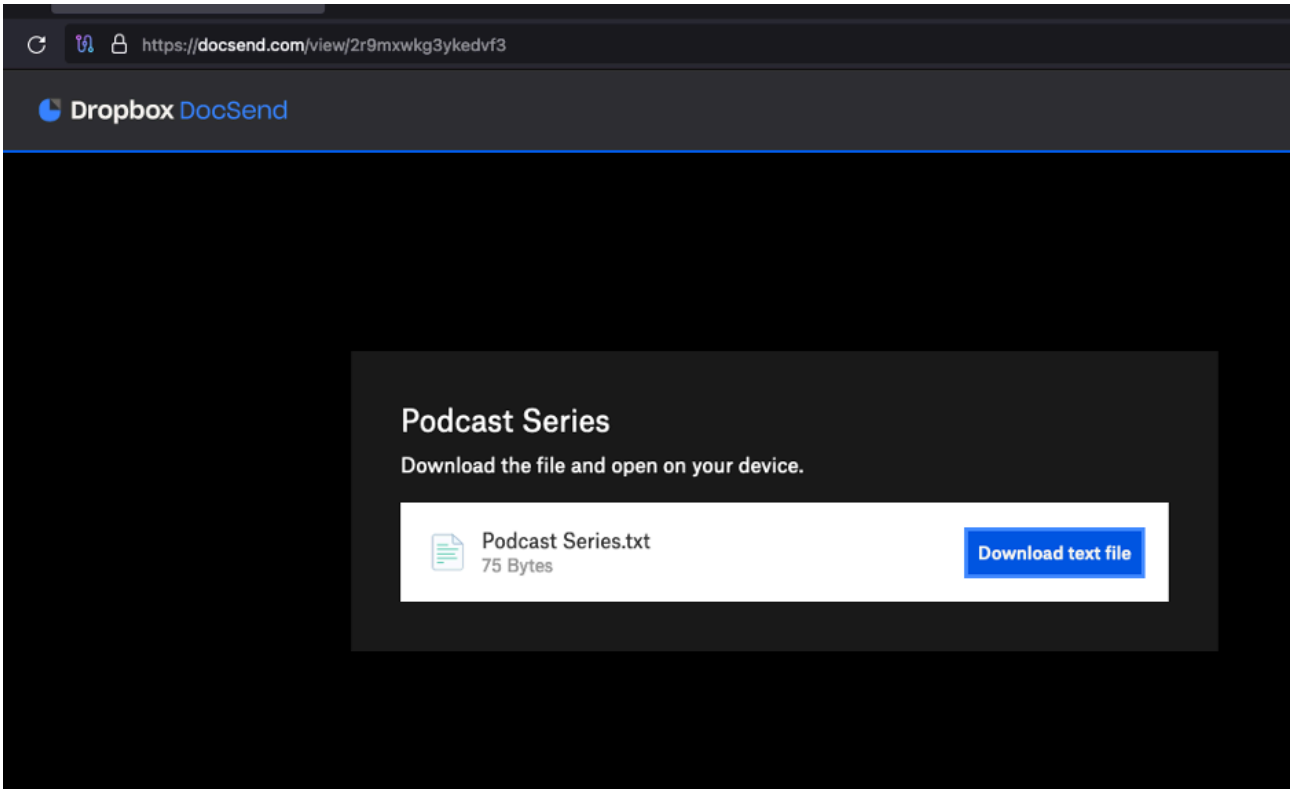
- Proofpoint identified Iranian threat actor TA453 targeting a prominent religious figure with a fake podcast interview invitation.
- The initial interaction attempted to lure the target to engage with a benign email to build conversation and trust to then subsequently click on a follow-up malicious link.
- The attack chain attempted to deliver a new malware toolkit called BlackSmith, which delivered a PowerShell trojan dubbed AnvilEcho by Proofpoint.
- The malware, which uses encryption and network communication techniques similar to previously observed TA453 samples, is designed to enable intelligence gathering and exfiltration.
- AnvilEcho contains all of TA453's previously identified malware capabilities in a single PowerShell script rather than the modular approach previously observed.

Overview

Starting 22 July 2024, TA453 contacted multiple email addresses for a prominent Jewish figure while pretending to be the Research Director for the Institute for the Study of War (ISW). The lure purported to invite the target to be a guest on a podcast hosted by ISW. After receiving a response from the target (outside of Proofpoint visibility), TA453 replied with a DocSend URL. The DocSend URL was password protected and led to a text file that contained a URL to the legitimate ISW Podcast being impersonated by TA453. It is likely that TA453 was attempting to normalize the target clicking a link and entering a password so the target would do the same when they delivered malware.



Initial July 2024 approach from TA453.



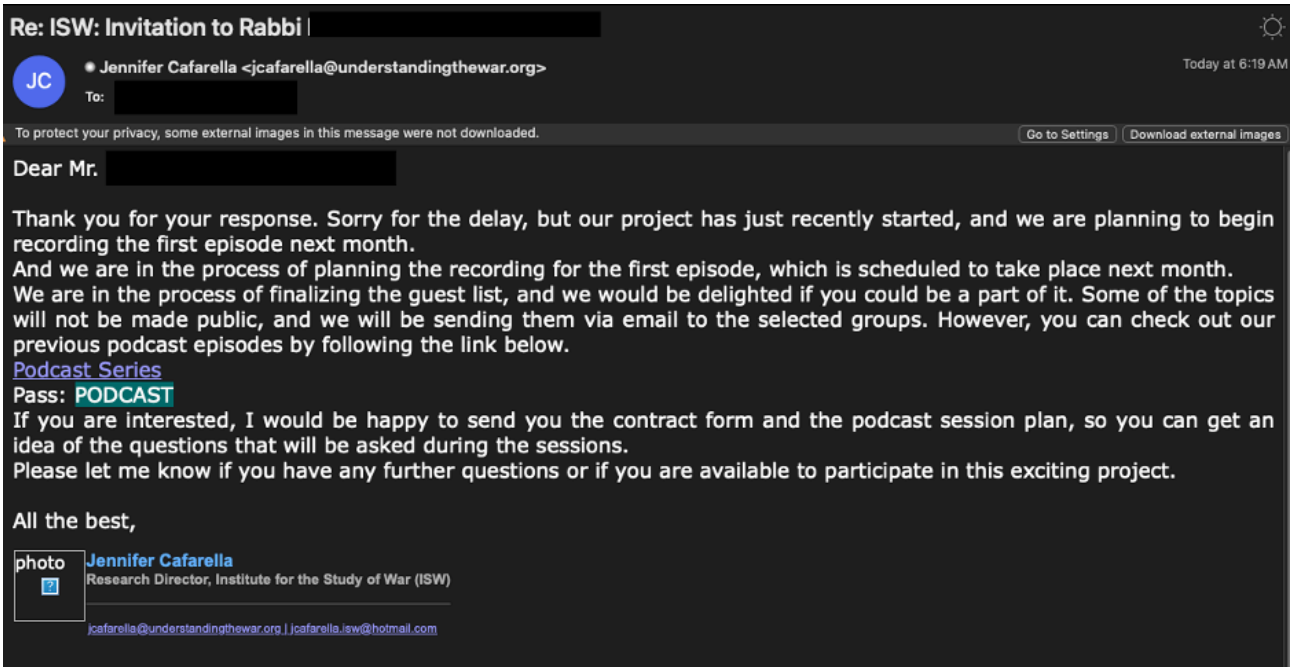
DocSend contents containing the podcast themed text.

Proofpoint first observed TA453 spoofing the Institute for the Study of War (ISW) in phishing campaigns targeting other organizations starting in February 2024, almost immediately after registering the domain in late January 2024. The theme of spoofing is consistent with broader TA453 phishing activity reported by Google Threat Intelligence Group in August 2024

TA453 initially sent the fake podcast invitation to the religious figure at multiple email accounts, specifically both the target's organizational email address along with their personal email address. Phishing multiple email addresses associated with a target has been observed by a number of state aligned threats, including TA427.

TA453 continued to establish their legitimacy by sending emails from understandingthewar[.]org and including a TA453 controlled Hotmail account in the email signature.

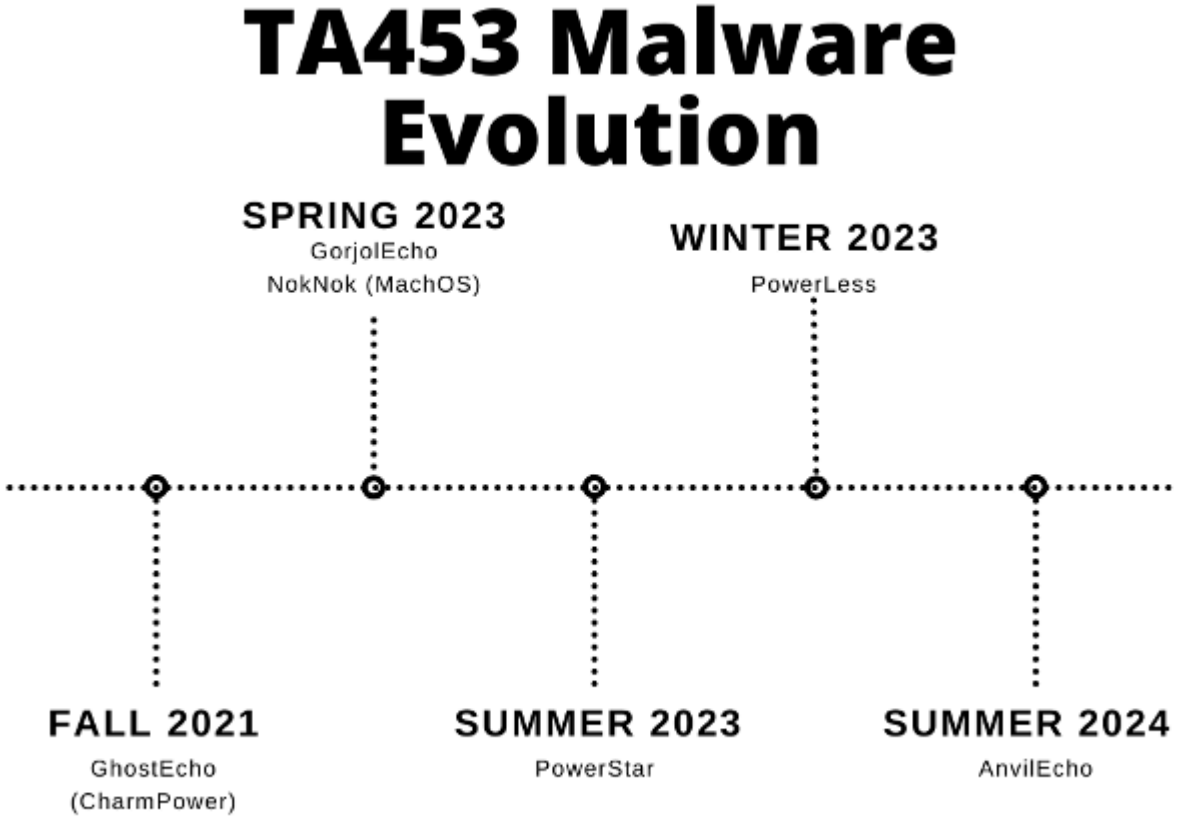
After another reply from the target, TA453 replied with a GoogleDrive URL leading to a ZIP archive named "Podcast Plan-2024.zip". The ZIP contained an LNK titled "Podcast Plan 2024.lnk". The LNK delivered the BlackSmith toolset which eventually loaded TA453's AnvilEcho Powershell Trojan.



Fake podcast invitation containing a malicious URL.

Malware analysis

Old habits die screaming, and TA453 sticks to its habits. Our analysis of the malware from this TA453 campaign demonstrates the developers working for TA453 have not given up on using modular PowerShell backdoors. They continue to attempt to evade detections by convoluting the infection chain in order to limit and avoid detection opportunities while collecting intelligence. The toolset observed in this infection chain is likely the successor of GorjolEcho/PowerStar, TAMECURL, MischiefTut, and CharmPower. The first TA453 backdoor was detected by Proofpoint in Fall 2021. Rather than deploy each Powershell module separately, TA453 attempts to bundle the entire framework into a single large PowerShell script dubbed AnvilEcho by Proofpoint.



Timeline of TA453 malware.

Infection chain

The LNK is used to smuggle additional files. It hides behind a decoy PDF as an overlay and extracts the contents of the ZIP folder to %TEMP%. The ZIP folder contains Beautifull.jpg, mary.dll, qemus (the encrypted AnvilEcho PowerShell script), soshi.dll, and toni.dll. A PDB path of E:\FinalStealer\blacksmith\blacksmith\ indicates the developers referred to the multi-component toolset written in C++ as “BlackSmith". This name was previously used by the TA453 POWERLESS browser stealer module as reported by Volexity . The browser stealer module is one of the capabilities included in the final stage of BlackSmith malware toolset.

PDF displayed to the user to obfuscate BlackSmith installation.

BlackSmith uses soshi.dll file as an installer, creating C:\Users\Public\Public Library and then copying mary.dll, qemus, and toni.dll. If qemus or toni.dll are not available, soshi.dll will download them from d75[.]site, a TA453 controlled storage site. The installer then extracts a file hidden with steganography as a base64 string inside Beautifull.jpg, a PNG file. Again, if the PNG file is not found in the working directory, it's downloaded from d75[.]site. After mary.dll is copied to the install folder, the installer registers toni.dll as a service for persistence.

Stage 2, toni.dll, is heavily obfuscated and starts by looking for antivirus installed on the system. If antivirus software is detected, the malware will rewrite the entry point of amsi.AmsiScanBuffer to force AmsiScanBuffer to return an Invalid Argument error when called. The same bypass is done for ntdll.EtwEventWrite. The stager then base64 decodes and AES/ECB decrypts qemus and launches videogui.exe, the PowerShell loader previously hidden in the PNG.

The next stage, the loader, loads the final stage, AnvilEcho. AnvilEcho is a PowerShell trojan that contains extensive functionality, including capabilities that expand on previous TA453 malware samples. TA453 developers attempted to bundle the previous capabilities of TA453 malware into a single PowerShell script. Previously, TA453 used individual scripts for each function of the malware, typically VBS or PowerShell scripts. Like NokNok, AnvilEcho repeatedly uses the same encryption and network communication functions across capabilities. Our analysis identified this AnvilEcho sample as version 3.2.3.

AnvilEcho starts by using System.Net.ServicePointManager to write TrustAllCertsPolicy, to bypass SSL Certificate Validation by forcing a system to accept all SSL/TLS certificates without validating them. Additionally, it extends the browser timeout, possibly to avoid disruption to long term command and control (C2) capabilities.

AnvilEcho uses deepspaceocean[.]info for C2 throughout the script. It checks for a previously generated MachineID in $env:PUBLIC\qwer.txt. The MachineID is computed in an unnecessarily complicated manner. If the MachineID does not already exist, AnvilEcho creates two random 32-character length alphanumeric strings and concatenates them. Afterwards, it takes that value and calculates the SHA256 hash of it before 16 characters from the hash are further concatenated with the original rand. This is then written to qwer.txt as a MachineID.

AnvilEcho consists of multiple functions, many of which are either similar to or improved on previously reported TA453 malware modules. The beginning of the script sets up a series of functions to encrypt, encode and exfiltrate information. These functions include Send-ReqPacket, FromEncrypt, From-Save, Encode, ToEncrypt, and Get-Rand. The design of using the same network communication and encryption functions across multiple modules is similar to what our analysis revealed in TA453's NokNok malware. Overall, AnvilEcho capabilities indicate a clear focus on intelligence collection and exfiltration.

The roughly 2200 lines of AnvilEcho PowerShell end with the two higher level functions of Redo-It and Do-It.

Redo-It overview

The Redo-It function serves as orchestration and management for all of the PowerShell in AnvilEcho. It processes commands from $Global:sacpath. In the analyzed sample, this is \Temp\stc. Additionally, Redo-It also handles key encryption. The first time Redo-It is run, it uses WMI to conduct system reconnaissance, looking to gather antivirus information, Operating System information, Public IP Address, InstallationPath, Manufacturer, ComputerName, and UserName. That information is then encrypted and sent to the TA453-controlled infrastructure. Designed to run continuously, Redo-It periodically fetches commands from the remote server, decrypts them, and executes them via Do-It.

Do-It overview

Based on the command received, Do-It executes different sections of code called out earlier in the PowerShell.

Command	Function	Notes

F_upload	First-Check	Network Connectivity
file_list	File-Handle	Looks for specified Path
shot	shotthis	Uses bitmap to screenshot, then converts to PNG which is then base64 encoded. Capability for multiple screens
sound	Get-Sound	Reads the contents of Applause.wav and then encodes them in base64 for exfiltration.
Browser	Get-WebInfo	
klg	Get-Stream	Allows for download of remote files, in a loop
Download	Get-From-Net	
Upload	Send-to-Net	Possible support for FTP and Dropbox uploading. Optional Parameters including password, chunking size and token
update	Config-Update	

Of note, additional troubleshooting functionality is included in AnvilEcho. The actor attempted to include IntelliSense, a code compilation aid, possibly in order to minimize detection opportunities from typos. In some cases, Sysinternals handl64 is downloaded if the actor is unable to access certain directories for over 20 seconds. Additionally, the script has code for downloading WinRAR and 7zip, similar to what was reported by Volexity. In this sample, it has been commented out of functionality. Finally, Send-Reqpacket is used for error handling in Do-It.

In addition to the network communication capabilities, AnvilEcho also includes code suggesting the actors have used both FTP and Dropbox for exfiltration in the past. This would be consistent with what Proofpoint previously observed along with third party industry reporting

TA453 used mary.dll as a helper very similar to toni.dll. It contained a single function called exFunc. This function allows for AES decryption followed by running the decrypted payloads in memory. The AES key is hardcoded.

Network analysis

As our analysis has demonstrated, d75[.]site is used for C2 by BlackSmith. This domain was reported as a URL shortener controlled by APT42 by Google Threat Intelligence Group in May 2024. It is cohosted on 54.39.143[.]117 with dropzilla.theworkpc[.]com, a suspected TA453 controlled host. TA453 previously utilized subdomains of theworkpc[.]com in previously reported campaigns from mid-2023.

Additionally, the AnvilEcho C2 server deepspaceocean[.]info, hosted on 54.39.143[.]120 bears similarities to historical TA453 infrastructure, including using OVH and .info TLD.

Attribution

These efforts likely support intelligence collection in support of Iranian government interests. While Proofpoint analysts cannot link TA453 directly to individual members of the Islamic Revolutionary Guard Corps (IRGC), Proofpoint does continue to assess that TA453 operates in support of the IRGC, specifically the IRGC Intelligence Organization (IRGC-IO). This assessment is based on a variety of evidence, including overlaps in unit numbering between Charming Kitten reports and IRGC units as identified by PWC, the US Department of Justice indictment of Monica Witt along with IRGC-affiliated actors, and analysis of TA453 targeting compared to reported IRGC-IO priorities. The IRGC, specifically the IRGC Intelligence Organization, collects intelligence and conducts operations in support of a variety of assigned responsibilities. This directive has led to targeting a series of diplomatic and political entities, ranging from embassies in Tehran to US political campaigns.

Proofpoint currently views TA453 as overlapping with Microsoft's Mint Sandstorm (formerly PHOSPHORUS) and roughly equivalent to Mandiant's APT42 and PWC's Yellow Garuda, all of which can generally be considered Charming Kitten.

Why it matters

TA453 uses many different social engineering techniques to try and convince targets to engage with malicious content. Like multi-persona impersonation, sending legitimate links to a target and referencing a real podcast from the spoofed organization can build user trust . When a threat actor builds a connection with a target over time before delivering the malicious payload, it increases the likelihood of exploitation.

With BlackSmith, TA453 has created a sophisticated intelligence collection toolkit and streamlined its malware functions from a disparate set of individual scripts into a full-service PowerShell trojan.

Emerging Threats signatures

2055244 - ET PHISHING TA453 Domain in DNS Lookup (deepspaceocean .info)
2055245 - ET PHISHING TA453 Domain in TLS SNI (deepspaceocean .info)

2055246 - ET PHISHING TA453 Domain in DNS Lookup (d75 .site) (phishing.rules)
2055247 - ET PHISHING TA453 Domain in TLS SNI (d75 .site) (phishing.rules)

Indicators of compromise

Indicator	Description	First Observed
5dca88f08b586a51677ff6d900234a1568f4474bbbfef258d59d73ca4532dcaf	SHA256 .LNK	2024-05-08
5aee7381210938664048 27e1db43c8e1a7882291afedfe90314ec90b198afb36	SHA256 Podcast Plan 2024.zip	2024-05-08
dc5c963f1428db051ff7aa4d43967a4087f9540a9d331dea616ca5013c6d67ce	SHA256 PDF	2024-05-08
dcb072061defd12f12deb659c66f40473a76d51c911040b8109ba32bb36504e3	Beautifull.jpg	2024-05-08
574fc53ba2e9684938d87fc486392568f8db0b92fb15028e441ffe26c920b4c5	mary.dll	2022-02-18
8a47fd166059e7e3c0c1740ea8997205f9e12fc87b1ffe064d0ed4b0bf7c2ce1	qemus (AnvilEcho)	2024-05-08
d033db88065bd4f548ed13287021ac899d8c3215ebc46fdd33f46a671bba731c	soshi.dll	2024-05-08
258d9d67e14506b70359daabebd41978c7699d6ce75533955736cdd2b8192c1a	toni.dll	2024-05-08

understandingthewar[.]org	Lure Domain	2024-02-01
d75[.]site	Storage/Stager	2024-03-04
deepspaceocean[.]info	C2	2024-02-22

Source: https://www.proofpoint.com/us/blog/threat-insight/best-laid-plans-ta453-targets-religious-figure-fake-podcast-invite-delivering