CERT-UA

General information

At the beginning of the fierce 2022, the CERT-UA Ukrainian Supervisory Computer Response Team, as one of the coordinating subjects, took away information about the detection of potentially scalable programs on the computers of spivrobitniks.

Based on the results of the analysis, it was established that the data on objects should be checked for the signs of shkidlivyh programs, classified as LightRope and LiteManager. Further correlation of indicators of compromise, as well as tactics, techniques and procedures, allowed the activity to be associated with the activities of the UAC-0008 group (Buhtrap). In view of the fact that the files of shkidlivih programs were signed with an electronic signature, the attack was specifically looked at before 01/16/2022.

Dovidkovo:

The Buhtrap group in the period from 2014 to 2016 recorded a low number of attacks , worse, on the financial organizations of Russia. At the same time, in 2016, in 2016, incl., after the publication of the victorious code of victorious programs, for unknown reasons, the group began to carry out attacks exclusively against specific state authorities and enterprises of Ukraine, victorious, in the middle, programmatically.

Depending on the nature of the injection on the information and telecommunication systems of the attacked organizations, it is obvious that the group is fixed in the corporate measure of sacrifice and the improvement of the process of taking away information, as it is processed in special systems of organizations.

For a preliminary demonstration of the method of penetration of that victorious group of instruments, it is important to visit the following incident, which may be the month of 2021.

So, apparently, for the help of electronic mail, the evil-doers created a rozposyudzhennya sending to the shkidly document “2021-07-30-08-55-07.xlsm”. Once the document is opened and the macro activated on the victim's computer, the file “output.exe” will be created, which is classified as the SourSnack program. Remaining with the basic information about the computer, generating a DNS-query to the control server, having removed the key from the output key, decoding the configuration file that was created at the resource looking at the configuration file and further decrypting the payload, which appears before the LightRope guesses (ale

Nadali, LightRope zdiysny dekoduvannya vbudovannogo resource, saving the file on the computer and the creation of a scheduled task to ensure the persistence of the launch of the rest. As a result, the dnscat program will be installed on the victim's computer to give the attackers the ability to remotely steal the add-on, tunneling information flows behind the DNS protocol.

Respectfully, that file-droppers, like vikoristovuyutsya group, as a rule, signed with a digital digital signature.

Not a crossover of shkidlivih programs that are victorious in a group:

dnscat - software security, spread out over various movable programs C. Designed to create an encrypted channel for managing between a client and a server behind an additional DNS protocol. Supported by *nix and Windows operating systems. Transferred functionality for remote viewing of commands on the client through the terminal.

LiteManager is a smartly cost-free program with a lock-out code for remote administration and computer management. Broken down by the Russian company LiteManagerTeam. The project is an official continuation of the closed Remote Office Manager project. The client part is available for operating systems: Windows, Android, Mac OS, iOS, iPhone, iPad.

SourSnack is a smart program, divided into different versions of C. It takes care of retrieving basic information about the computer (GetComputerName, GetUserName, GetAdaptersInfo). There is a connection with the management server for decrypting the encryption key for decrypting the PE file, which is located at the encrypted resource, and saving it on the computer in the %APPDATA% directory and further launch. For communication with the control server, the DNS protocol (TXT records) is used; Information about EOM is encoded for help hex. To decrypt the resource, XOR is required; for decryption of a PE file, an algorithm based on mathematical operations (XOR / DIV / MUL) is used, which implements the transformation of blocks, the majority of which is assigned the encryption key.

LightRope is a tricky program, divided into different versions of C. It takes the role of a dropper, allowing ZLIB decompression (may not be broken) and XOR decoding of the payload of the resource, as well as the creation of a scheduled task. With the method of unification of the created files, the elements of their resources can be filled with sufficient tribute.

NTDSDumpEx is a publicly available security software, recognized for extracting information from the Active Directory database %SYSTEMROOT%\NTDS.dit, and itself: data about domain cloud records, group memberships and password hashes.

RDPWrapper is a publicly available security software designed to make it possible to run multiple parallel RDP sessions on a computer.

Ngrok is a publicly available software, recognized for the publication of any service (meadow port) on the Internet through the tunneling of information flows.

Indicators of compromise

Files:

```
1b5f0425dd76496e715bfa1aa76d306c facebook.exe (LightRope)
42397efeaf1d971896cdc91ca024974d lsass.exe (LiteManager)
9297e47fe1b256a8bbcb2b7a20844b2c svchost.exe (LiteManager)
42397efeaf1d971896cdc91ca024974d lsass.exe (LiteManager)
43a9a42b9a656d1ca39a3337a841ad5d NTDSDumpEx.exe (NTDSDumpEx)
c1f47a14a958e2345ba929afa829c7e7 2021-07-30-08-55-07.xlsm
```

86926e56e4f6d854161066b5989a350e output.exe (SourSnack)
3dcec8f6ba15e801b63b7c21a6b966fb dnsoption.exe (LightRope_v2)
86f322fe52829b8b8094d053ed648a65 CDSSyncReporting.exe (dnscat)

Merezhev:

hxxps://mail.nais-gov[.]org/2021-07-30-08-55-07.xlsm
widget.forum-pokemon[.]com
ns.ns2-dns[.]com
ns.ns3-dns[.]com
ns3-dns[.]com
ns2-dns[.]com
cs1.wpc-v0cdn[.]org
wpc-v0cdn[.]org
ipv6-wpnc[.]net
alt-2cdn[.]net
nais-gov[.]org
nais-gov[.]com
91[.]240.86.200
89[.]108.101.61
45[.]76.85.232
185[.]162.9.218
95[.]179.135.36
91[.]240.86.200:5651

Hosts:

Mikael LLC (administrator@mikael-company[.]ru)
George Alan Developments Incorporated

C:\windows\system32\wbem\wmic.exe process where ExecutablePath='C:\\ProgramData\\lsass.exe' delete
C:\windows\system32\wbem\wmic.exe process where ExecutablePath='C:\\ProgramData\\svchost.exe' delete
C:\windows\system32\schtasks.exe /delete /tn "Network Security Update" /f
C:\windows\system32\schtasks.exe /create /sc onstart /tn "Network Security Update" /tr "C:\ProgramData\lsass.exe" /en SYSTEM
%PROGRAMDATA%\lsass.exe
%PROGRAMDATA%\svchost.exe
%PROGRAMDATA%\config.xml
%PUBLIC%\output.exe
%APPDATA%\dnsoption.exe
%APPDATA%\Microsoft\Windows\CDSSyncReporting.exe

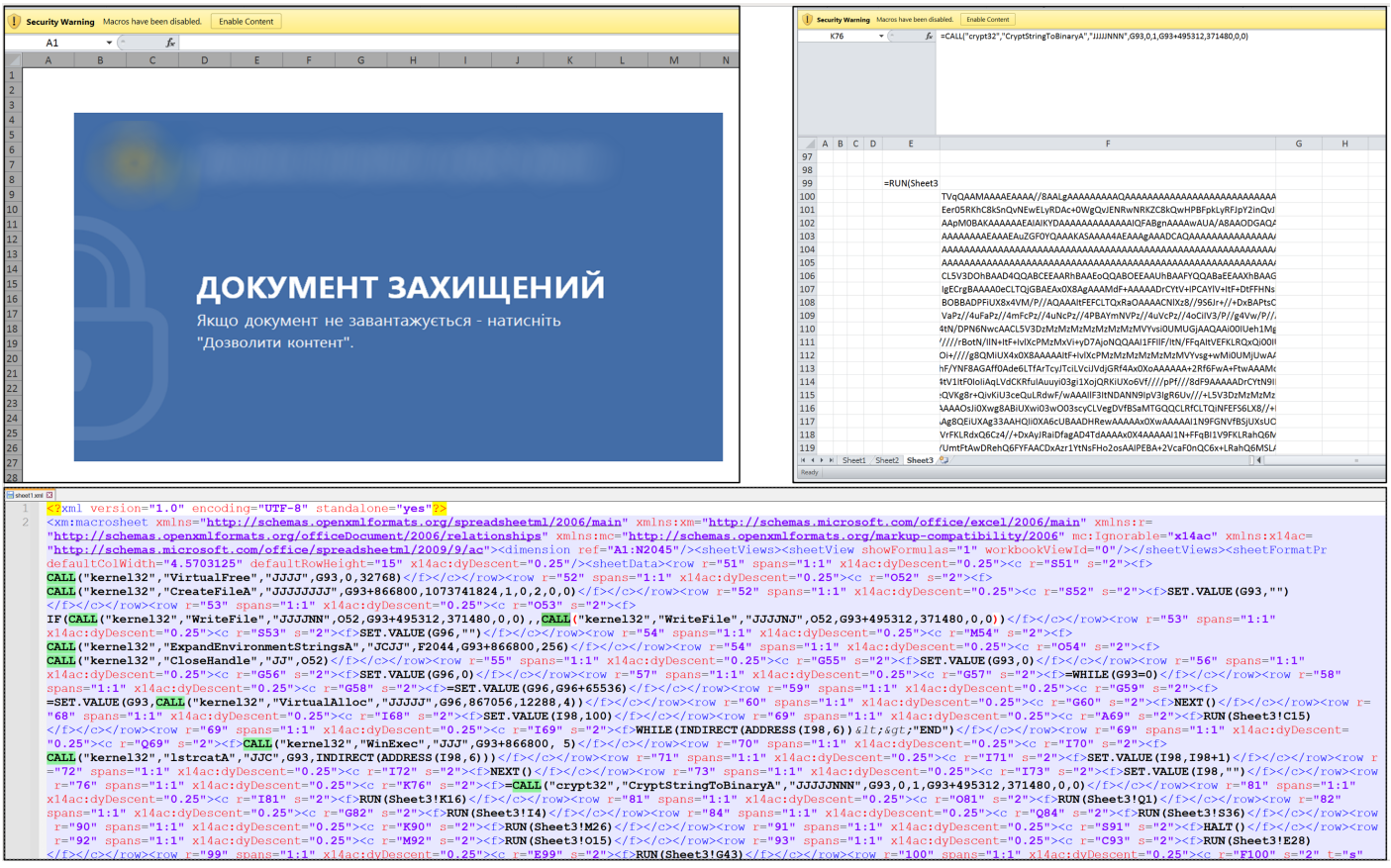
Additional information

· It is recommended to change the so-called “attack surface” (attack surface), including for filtering mesh ports for external information flows.

· With the method of revealing the facts of tunneling information flows behind the additional DNS protocol, perform rechecking and further monitoring of the log files for the presence of anomalous DNS backlogs.

· Implement the possibility of centralized management of anti-virus protection on all non-powered computers; transfer the ability to live on computers (launching Yara-rules, accessing shkidlivih files, searching for indicators then), in the first line, in remote access mode.

Graphic images



Rice. 1 Download free download