In the Balkans, businesses are under fire from a double-barreled weapon

welivesecurity.com/2019/08/14/balkans-businesses-double-barreled-weapon

August 14, 2019

ESET researchers discovered a campaign that uses two malicious tools with similar capabilities to ensure both resilience and broader potential for the attackers

Zuzana Hromcová 14 Aug 2019 - 11:30AM

We've discovered an ongoing campaign in the Balkans spreading two tools having a similar purpose: a backdoor and a remote access trojan we named, respectively, BalkanDoor and BalkanRAT.

BalkanRAT enables the attacker to remotely control the compromised computer via a graphical interface, i.e., manually; BalkanDoor enables them to remotely control the compromised computer via a command line, i.e., possibly *en masse*. ESET security products detect these threats as Win{32,64}/BalkanRAT and Win32/BalkanDoor.

A typical victim of this campaign, which uses malicious emails as its spreading mechanism, ends up having both these tools deployed on their computer, each of them capable of fully controlling the affected machine. This rather uncommon setup makes it possible for attackers to choose the most suitable method to instruct the computer to perform operations of their choice.

The campaign's overarching theme is taxes. With the contents of the emails, included links and decoy PDFs all involving taxes, the attackers are apparently targeting the financial departments of organizations in the Balkans region. Thus, although backdoors and other tools for remote access are often used for espionage, we believe that this particular campaign is financially motivated.

The campaign has been active at least from January 2016 to the time of writing (the most recent detections in our telemetry are from July 2019). Some parts of the campaign were briefly described by a Serbian security provider in 2016 and the Croatian CERT in 2017. Each of these sources focused only on one of the two tools and only on a single country. However, our research shows that there is a significant overlap in targets and also in the attackers' tactics, techniques and procedures.

Our findings show that the mentioned attacks have been orchestrated and we consider them a single long-term campaign that spans Croatia, Serbia, Montenegro, and Bosnia and Herzegovina.

Our research has also shed more light at the malware used in this campaign and provided some context. We've discovered a new version of BalkanDoor with a new method for execution/installation: an exploit of the WinRAR ACE vulnerability (CVE-2018-20250). Further, we've seen both malicious tools digitally signed with various certificates the developers paid for to add perceived legitimacy. One of them, issued to SLOW BEER LTD, was even valid at the time of writing; we've notified the issuer about the misuse and they revoked the certificate.

In this article, we will describe some notable features of both BalkanDoor and BalkanRAT. Our analysis shows that the former runs as a Windows service, which allows it to unlock the Windows logon screen remotely and without the password or start a process with the highest possible privileges. The latter misuses a legitimate remote desktop software (RDS) product and uses extra tools and scripts to hide its presence from the victim, such as hiding the window, tray icon, process and so on.

Targets and distribution

Both BalkanRAT and BalkanDoor spread in Croatia, Serbia, Montenegro, and Bosnia and Herzegovina. (These countries, along with Slovenia and former Macedonia, formed the country of Yugoslavia until 1992.)

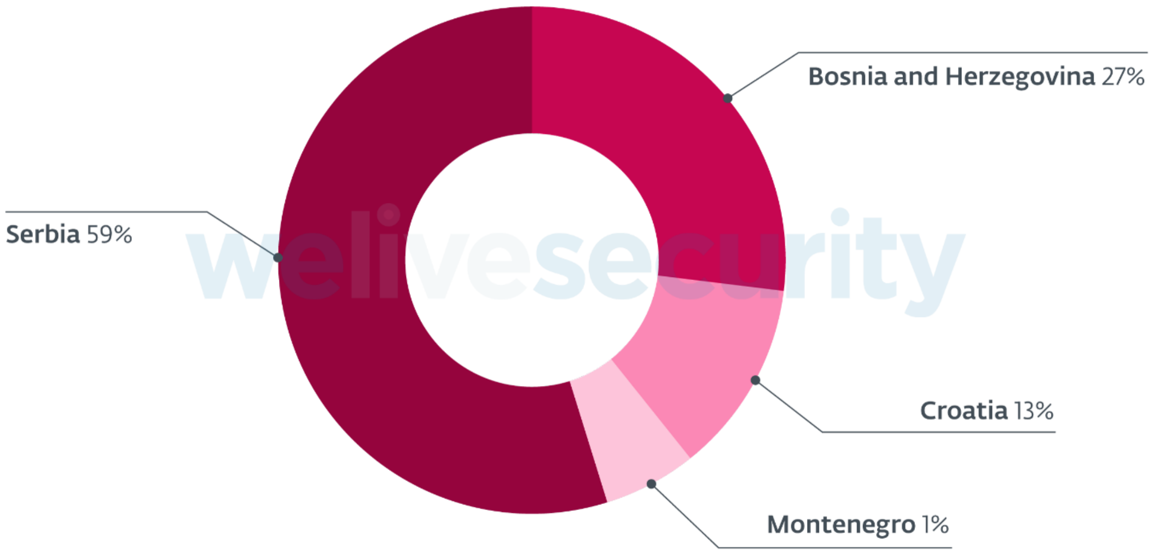


Figure 1. Malware distribution by country

According to our telemetry, the campaign spreading these tools has been live since 2016, with the most recent detections as late as in July 2019.

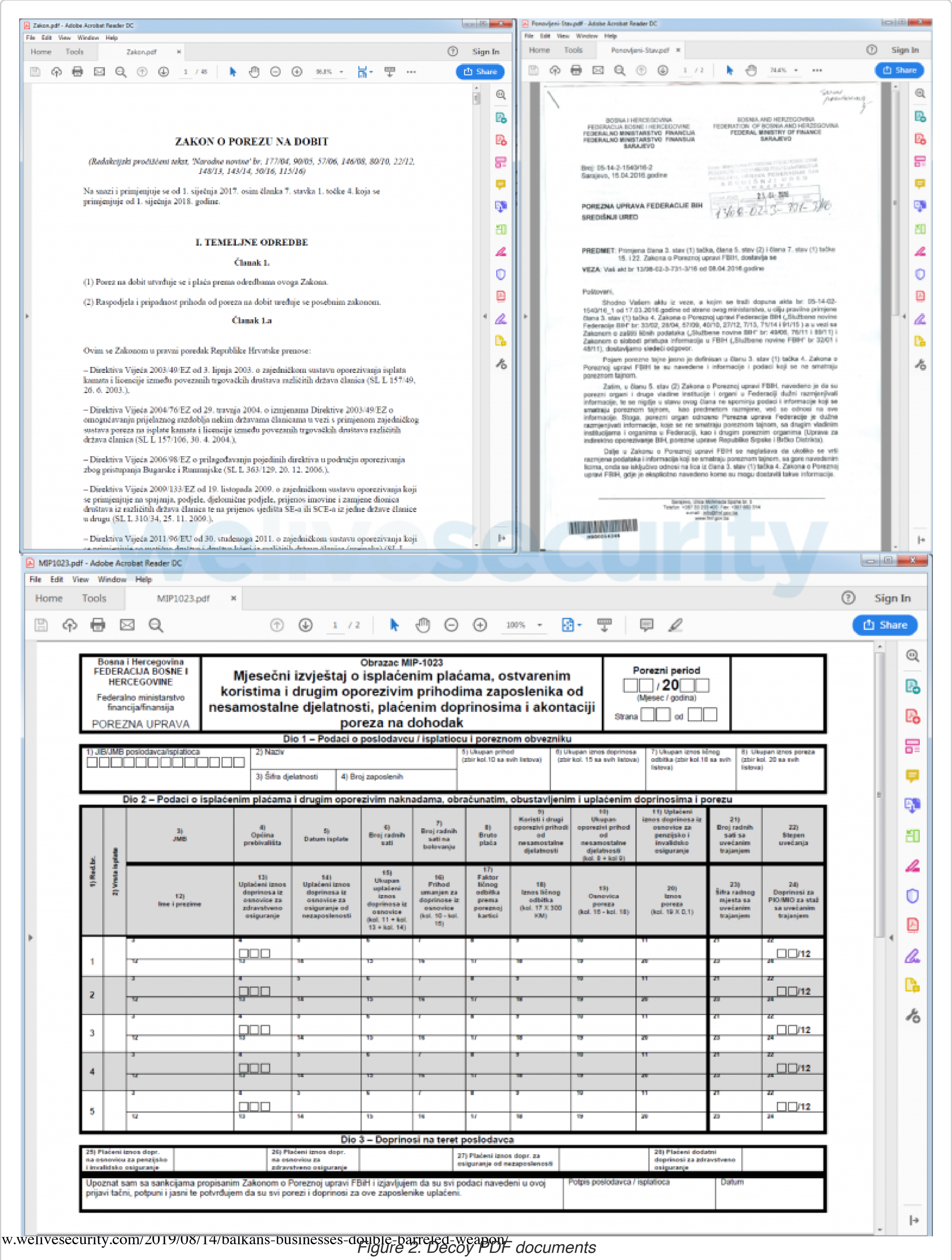
The attackers have been distributing their tools via malicious emails (“malspam”) with links leading to a malicious file.

The links included in the malspam emails used for distribution of both BalkanRAT and BalkanDoor mimic legitimate websites of official institutions.

Malicious domain	Real domain	Institution
pksrs[.]com	pks.rs	Chamber of Commerce and Industry of Serbia
porezna-uprava[.]com	porezna-uprava.hr	Ministry of Finance of Croatia, Tax Administration
porezna-uprava[.]net		
pufbih[.]com	pufbih.ba	Tax Administration of the Federation of Bosnia and Herzegovina

The decoy PDFs revolve around the tax theme

PDF name	Language	Content
MIP1023.pdf	Bosnian	Tax form
Ponovljeni-Stav.pdf	Bosnian	Tax law
AUG_1031.pdf	Bosnian	Instructions for using tax filing application
Zakon.pdf	Croatian	Tax law
ZPDG.pdf	Serbian	Tax law



Zakon.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools Zakon.pdf
Sign In
1 / 48
96,8%
Share

ZAKON O POREZU NA DOBIT

(Redakcijski pročišćeni tekst, 'Narodne novine' br. 177/04, 90/05, 57/06, 146/08, 80/10, 22/12, 148/13, 143/14, 50/16, 115/16)

Na snazi i primjenjuje se od 1. siječnja 2017. osim članka 7. stavka 1. točke 4. koja se primjenjuje od 1. siječnja 2018. godine.

I. TEMELJNE ODREDBE

Članak 1.

(1) Porez na dobit utvrđuje se i plaća prema odredbama ovoga Zakona.

(2) Raspodjela i pripadnost prihoda od poreza na dobit uređuje se posebnim zakonom.

Članak 1.a

Ovim se Zakonom u pravni poredak Republike Hrvatske prenose:

– Direktiva Vijeća 2003/49/EZ od 3. lipnja 2003. o zajedničkom sustavu oporezivanja isplata kamata i licencije između povezanih trgovačkih društava različitih država članica (SL L 157/49, 26. 6. 2003.),

– Direktiva Vijeća 2004/76/EZ od 29. travnja 2004. o izmjenama Direktive 2003/49/EZ o omogućavanju prijelaznog razdoblja nekim državama članicama u vezi s primjenom zajedničkog sustava poreza na isplate kamata i licencije između povezanih trgovačkih društava različitih država članica (SL L 157/106, 30. 4. 2004.),

– Direktiva Vijeća 2006/98/EZ o prilagođavanju pojedinih direktiva u području oporezivanja zbog pristupanja Bugarske i Rumunjske (SL L 363/129, 20. 12. 2006.),

– Direktiva Vijeća 2009/133/EZ od 19. listopada 2009. o zajedničkom sustavu oporezivanja koji se primjenjuje na spajanja, podjele, djelomične podjele, prijenos imovine i zamjene dionica društava iz različitih država članica te na prijenos sjedišta SE-a ili SCE-a iz jedne države članice u drugu (SL L 310/34, 25. 11. 2009.),

– Direktiva Vijeća 2011/96/EU od 30. studenoga 2011. o zajedničkom sustavu oporezivanja koji

Ponovljeni-Stav.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools Ponovljeni-Stav.pdf
Sign In
1 / 2
74,4%
Share

BOSNA I HERCEGOVINA
FEDERACIJA BOSNE I HERCEGOVINE
FEDERALNO MINISTARSTVO FINANCIJA
FEDERALNO MINISTARSTVO FINANSIJA
SARAJEVO

BOSNIA AND HERZEGOVINA
FEDERATION OF BOSNIA AND HERZEGOVINA
FEDERAL MINISTRY OF FINANCE
SARAJEVO

Broj: 05-14-2-1540/16-2
Sarajevo, 15.04.2016.godine

SREDIŠNJI URED
SARAJEVO
23. 04. 2016
13/08-02-3-731-3/16

POREZNA UPRAVA FEDERACIJE BIH
SREDIŠNJI URED

PREDMET: Primjena člana 3. stav (1) tačka, člana 5. stav (2) i člana 7. stav (1) tačke 15. i 22. Zakona o Poreznoj upravi FBiH, dostavlja se

VEZA: Vaš akt br 13/08-02-3-731-3/16 od 08.04.2016.godine

Poštovani,

Shodno Vašem aktu iz veze, a kojim se traži dopuna akta br: 05-14-02-1540/16_1 od 17.03.2016.godine od strane ovog ministarstva, u cilju pravilne primjene člana 3. stav (1) tačka 4. Zakona o Poreznoj upravi Federacije BiH („Službene novine Federacije BiH" br: 33/02, 28/04, 57/09, 40/10, 27/12, 7/13, 71/14 i 91/15) a u vezi sa Zakonom o zaštiti ličnih podataka („Službene novine BiH" br: 49/06, 76/11 i 89/11) i Zakonom o slobodi pristupa informacija u FBiH („Službene novine FBiH" br 32/01 i 48/11), dostavljamo slijedeći odgovor.

Pojam porezne tajne jasno je definisan u članu 3. stav (1) tačka 4. Zakona o Poreznoj upravi FBiH te su navedene i informacije i podaci koji se ne smatraju poreznom tajnom.

Zatim, u članu 5. stav (2) Zakona o Poreznoj upravi FBiH, navedeno je da su porezni organi i druge vladine institucije i organi u Federaciji dužni razmjenjivati informacije, te se nigdje u stavu ovog člana ne spominju podaci i informacije koji se smatraju poreznom tajnom, kao predmetom razmjene, već se odnosi na sve informacije. Stoga, porezni organ odnosno Porezna uprava Federacije je dužna razmjenjivati informacije, koje se ne smatraju poreznom tajnom, sa drugim vladinim institucijama i organima u Federaciji, kao i drugim poreznim organima (Uprava za indirektno oporezivanje BiH, porezne uprave Republike Srpske i Brčko Distrikta).

Dalje u Zakonu o Poreznoj upravi FBiH se naglašava da ukoliko se vrši razmjena podataka i informacija koji se smatraju poreznom tajnom, sa gore navedenim licima, onda se isključivo odnosi na lica iz člana 3. stav (1) tačka 4. Zakona o Poreznoj upravi FBiH, gdje je eksplicitno navedeno kome su mogu dostaviti takve informacije.

Sarajevo, Ulica Mehmeda Spahe br. 5
Telefon: +387 33 253-400 Fax: +387 660 314
e-mail: info@fmf.gov.ba
www.fmf.gov.ba

MIP1023.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools MIP1023.pdf
Sign In
1 / 2
100%
Share

Bosna i Hercegovina FEDERACIJA BOSNE I HERCEGOVINE Federalno ministarstvo financija/finansija POREZNA UPRAVA	Obrazac MIP-1023 **Mjesečni izvještaj o isplaćenim plaćama, ostvarenim koristima i drugim oporezivim prihodima zaposlenika od nesamostalne djelatnosti, plaćenim doprinosima i akontaciji poreza na dohodak**	**Porezni period** □□ / 20□□ (Mjesec / godina) Strana □□ od □□

Dio 1 – Podaci o poslodavcu / isplatiocu i poreznom obvezniku

1) JIB/JMB poslodavca/isplatioca □□□□□□□□□□□□□	2) Naziv		5) Ukupan prihod (zbir kol.10 sa svih listova)	6) Ukupan iznos doprinosa (zbir kol. 15 sa svih listova)	7) Ukupan iznos ličnog odbitka (zbir kol.18 sa svih listova)	8) Ukupan iznos poreza (zbir kol. 20 sa svih listova)
	3) Šifra djelatnosti	4) Broj zaposlenih				

Dio 2 – Podaci o isplaćenim plaćama i drugim oporezivim naknadama, obračunatim, obustavljenim i uplaćenim doprinosima i porezu

1) Red.br.	2) Vrsta isplate	3) JMB	4) Općina prebivališta	5) Datum isplate	6) Broj radnih sati	7) Broj radnih sati na bolovanju	8) Bruto plaća	9) Koristi i drugi oporezivi prihodi od nesamostalne djelatnosti	10) Ukupan oporezivi prihod od nesamostalne djelatnosti (kol. 8 + kol 9)	11) Uplaćeni iznos doprinosa iz osnovice za penzijsko i invalidsko osiguranje	21) Broj radnih sati sa uvećanim trajanjem	22) Stepen uvećanja
		12) Ime i prezime	13) Uplaćeni iznos doprinosa iz osnovice za zdravstveno osiguranje	14) Uplaćeni iznos doprinosa iz osnovice za osiguranje od nezaposlenosti	15) Ukupan uplaćeni iznos doprinosa iz osnovice (kol. 11 + kol. 13 + kol. 14)	16) Prihod umanjen za doprinose iz osnovice (kol. 10 - kol. 15)	17) Faktor ličnog odbitka prema poreznoj kartici	18) Iznos ličnog odbitka (kol. 17 X 300 KM)	19) Osnovica poreza (kol. 16 - kol. 18)	20) Iznos poreza (kol. 19 X 0,1)	23) Šifra radnog mjesta sa uvećanim trajanjem	24) Doprinosi za PIO/MIO za staž sa uvećanim trajanjem
1		3 12	4 □□□ 13	5 14	6 15	7 16	8 17	9 18	10 19	11 20	21 23	22 □□/12 24
2		3 12	4 □□□ 13	5 14	6 15	7 16	8 17	9 18	10 19	11 20	21 23	22 □□/12 24
3		3 12	4 □□□ 13	5 14	6 15	7 16	8 17	9 18	10 19	11 20	21 23	22 □□/12 24
4		3 12	4 □□□ 13	5 14	6 15	7 16	8 17	9 18	10 19	11 20	21 23	22 □□/12 24
5		3 12	4 □□□ 13	5 14	6 15	7 16	8 17	9 18	10 19	11 20	21 23	22 □□/12 24

Dio 3 – Doprinosi na teret poslodavca

25) Plaćeni iznos dopr. na osnovicu za penzijsko i invalidsko osiguranje		26) Plaćeni iznos dopr. na osnovicu za zdravstveno osiguranje		27) Plaćeni iznos dopr. za osiguranje od nezaposlenosti		28) Plaćeni dodatni doprinosi za zdravstveno osiguranje	

Upoznat sam sa sankcijama propisanim Zakonom o Poreznoj upravi FBiH i izjavljujem da su svi podaci navedeni u ovoj prijavi tačni, potpuni i jasni te potvrđujem da su svi porezi i doprinosi za ove zaposlenike uplaćeni.	Potpis poslodavca / isplatioca	Datum

Figure 2. Decoy PDF documents

Most often, the links leading to an executable file are disguised as links to a PDF. The executable file is a WinRAR self-extractor with its name and icon changed to resemble a PDF to fool the user. When executed, it is configured to unpack its content, open the decoy PDF to prevent any suspicion – and silently execute either BalkanRAT or BalkanDoor.

In some of the latest samples of BalkanDoor detected in 2019, the malware is distributed as an ACE archive, disguised as a RAR archive (i.e., not an executable file), specially crafted to exploit the WinRAR ACE vulnerability (CVE-2018-20250). This vulnerability, which has been remediated in version 5.70 released on February 28th, 2019, is known to have been exploited quite often to distribute malware.

The exploit-based deployment of BalkanDoor is stealthier than in previous versions of the malware because it does not require executing the downloaded file – an operation that might raise the intended victim's suspicions.

The campaign

According to our telemetry, most of the time, both tools have been deployed on the same machine. The combination of the tools gives the attacker both a command-line interface and a graphical interface to the compromised computer.

In the case of the whole toolset being deployed on the machine, here is an example scenario for the attack:

The attacker detects that the victim has their screen locked and thus, most probably, is not using the computer (either via BalkanDoor sending screenshot showing that computer is locked, or via the View Only mode of BalkanRAT). Via the BalkanDoor backdoor, the attacker sends a backdoor command to unlock the screen… and using BalkanRAT, they can do whatever they want on the computer.

However, even if the victim does not use their computer, the chance of them spotting the actions performed by the attackers is still there. Even with this disadvantage, using the RDS tool may be useful. The attacker is not limited by the commands shipped in the backdoor, or by their programming skills: manually, they can perform actions that would require writing a lot of code if a backdoor was the only tool available.

In principle, the Balkan- toolset could be used for espionage, among other possible goals. However, not only the campaign's targets and distribution, but also our analysis of the Balkan-toolset tools show that the attackers are going after money instead of espionage.

The BalkanDoor backdoor does not implement any exfiltration channel. Presumably, if the campaign were intended for espionage, the attackers would need an exfiltration channel for uploading the collected data – at least as a backup to manual exfiltration, which might not be always an option.

On the contrary – and supporting the notion that the attackers' goal has been to commit some financial crime – we've seen BalkanRAT dropping a tool that can list available smart cards, via the SCardListReadersA/ SCardConnectA API functions. Smart cards are usually issued by banks or governments for confirmation of the holder's identity. If misused, smart cards can facilitate illegal/fraudulent activities, e.g. digitally signing a contract, validating a money transaction etc.

In the past, we've seen this feature in Operation Buhtrap, a campaign targeting Russian banks.

Analysis – BalkanDoor

BalkanDoor is a simple backdoor with a small number of commands (download and execute a file, create a remote shell, take a screenshot). It can be used to automate tasks on the compromised computer or to automatically control several affected computers at once. We have seen six versions of the backdoor, ranging in supported commands, evolving since 2016.

The initial dropper unpacks all components, opens a decoy PDF (in some cases) and executes a batch installation script that ensures persistence of the backdoor.

The backdoor registers itself as a service, under a legitimately-looking service name (e.g. WindowsSvc, WindowsPrnt, WindowsConn or WindowsErr); the accompanying batch scripts can further ensure persistence by using Registry Run Keys or Startup folder.

After the backdoor is installed, the computer connects to a C&C server, identifying itself by the computer name and requesting the commands. The backdoor can connect to any of the C&Cs from a hardcoded list – a measure to increase resilience. It connects via the HTTP or HTTPS protocol; if HTTPS is used, then the server certificates are ignored.

If the connection is not successful, the backdoor is capable of using the user-configured proxy on the victim's computer and repeating the connection attempt.

The backdoor commands come in a format of an INI file, with properties determining the commands, command arguments and intended recipients. Specifying the list of recipients allows the attacker to send their commands to several compromised computers at once, e.g. to automatically take screenshots of all compromised computers.

Commands	Functionality
cn	Specifies computer name(s) of the intended recipients of the commands
du, int	Download and execute a file
du, ra, de, rpo	Download and execute a file, in the specified context and on a specified desktop
rip	Create a remote shell accessible from the specified IP address
scr_int, scr_dur	Capture a series of screenshots of the specified duration

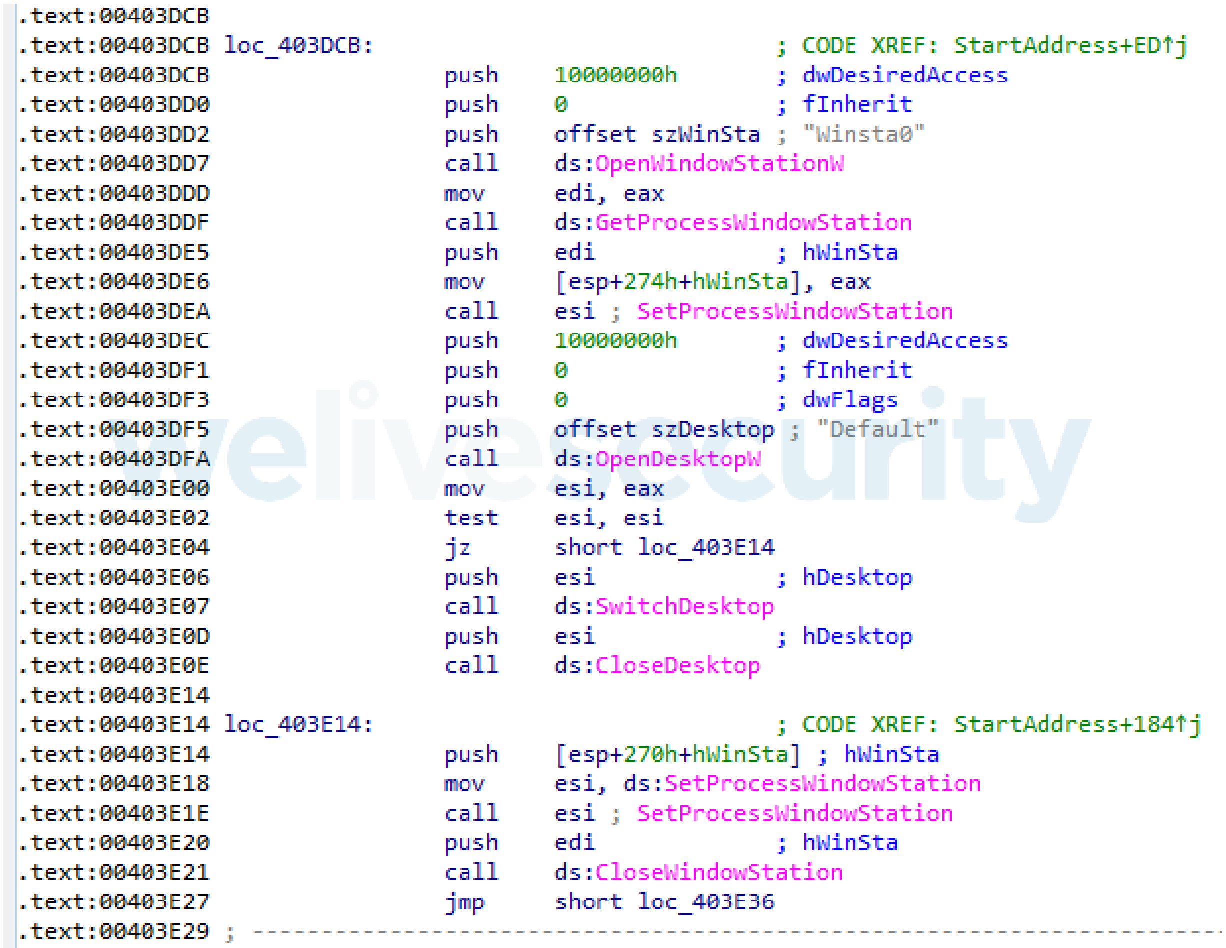
Furthermore, the backdoor itself can be executed in several modes, determined by the command line arguments with which it is executed. These modes themselves can serve as backdoor commands (when executed from the remote shell):

Argument	Functionality
/unlock	Unlocks the screen
/rcmd	Creates a remote shell and redirects its input/output to the specified IP address
/takescr	Captures a series of screenshots, duration determined by other arguments
/run	Executes the specified command using cmd.exe
/runx	Executes the specified command using cmd.exe, on the active (input) desktop
/inst	Installs itself as a service and starts the main procedure (see /nosvc)

/start	Starts the associated service, which starts the main procedure (see /nosvc)
/nosvc	Main payload, communicates with C&C and interprets backdoor commands

Among the BalkanDoor capabilities, the most notable is passwordless screen-unlocking.

This feature comes in handy to the attackers in cases when a logged-in user locks the computer. The “Lock screen” is just another Desktop for the system, so any malware with the necessary privileges can switch to a real desktop by command. No password is required to perform this operation.



```
.text:00403DCB
.text:00403DCB loc_403DCB:                             ; CODE XREF: StartAddress+ED↑j
.text:00403DCB                 push    10000000h       ; dwDesiredAccess
.text:00403DD0                 push    0               ; fInherit
.text:00403DD2                 push    offset szWinSta ; "Winsta0"
.text:00403DD7                 call    ds:OpenWindowStationW
.text:00403DDD                 mov     edi, eax
.text:00403DDF                 call    ds:GetProcessWindowStation
.text:00403DE5                 push    edi             ; hWinSta
.text:00403DE6                 mov     [esp+274h+hWinSta], eax
.text:00403DEA                 call    esi ; SetProcessWindowStation
.text:00403DEC                 push    10000000h       ; dwDesiredAccess
.text:00403DF1                 push    0               ; fInherit
.text:00403DF3                 push    0               ; dwFlags
.text:00403DF5                 push    offset szDesktop ; "Default"
.text:00403DFA                 call    ds:OpenDesktopW
.text:00403E00                 mov     esi, eax
.text:00403E02                 test    esi, esi
.text:00403E04                 jz      short loc_403E14
.text:00403E06                 push    esi             ; hDesktop
.text:00403E07                 call    ds:SwitchDesktop
.text:00403E0D                 push    esi             ; hDesktop
.text:00403E0E                 call    ds:CloseDesktop
.text:00403E14
.text:00403E14 loc_403E14:                             ; CODE XREF: StartAddress+184↑j
.text:00403E14                 push    [esp+270h+hWinSta] ; hWinSta
.text:00403E18                 mov     esi, ds:SetProcessWindowStation
.text:00403E1E                 call    esi ; SetProcessWindowStation
.text:00403E20                 push    edi             ; hWinSta
.text:00403E21                 call    ds:CloseWindowStation
.text:00403E27                 jmp     short loc_403E36
.text:00403E29 ; ---------------------------------------------------------------------------
```

Figure 3. Code responsible for unlocking the computer when the backdoor is executed remotely with an “/unlock” argument

Analysis – BalkanRAT

The BalkanRAT part of the malicious Balkan- toolset is more complex compared to its backdoor accomplice. Its goal is to deploy a copy of the Remote Utilities software, which is commercial software by a Russian vendor, Remote Utilities, LLC, used for remote access to a computer or for remote administration. BalkanRAT also provides the attacker with the credentials needed for this remote access.

BalkanRAT has several additional components to help load, install and conceal the existence of the RDS. They can add exceptions to the firewall, hide the RDS’s window and its tray icon, and hide the presence of related processes in the task manager.

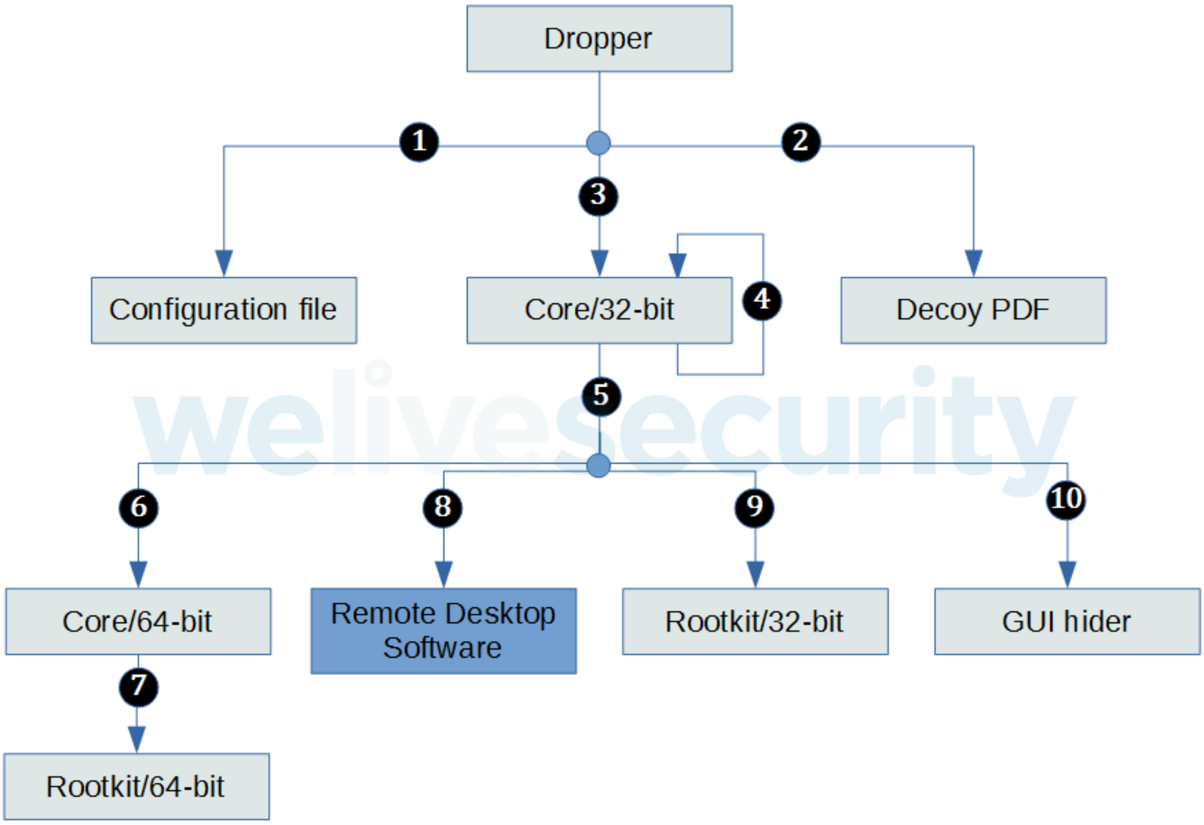


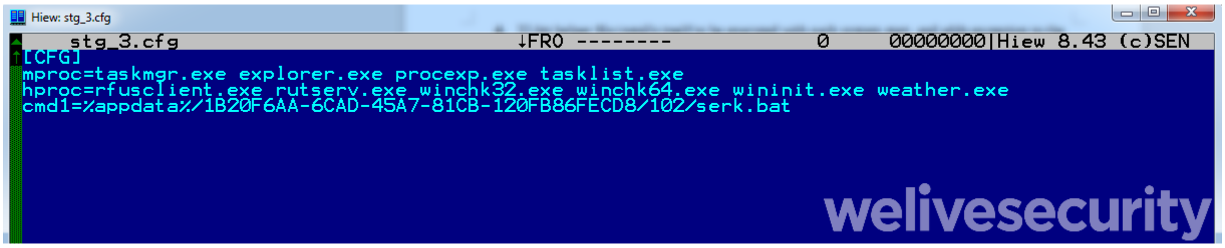
Figure 4. Components used in the campaign to deploy and hide the presence of the RDS

1. The dropper first unpacks all components; a configuration file, the remote desktop software and a core component installing it, a userland rootkit, a GUI hider and a decoy PDF file.
2. The dropper opens the PDF file so as not to arouse suspicion of the user.
3. Covertly, the dropper executes the core component (32-bit) in the installation mode.
4. The core component (32-bit) installs itself to be executed with each start, and adds exception to the firewall for the RDS. It executes commands inst1 and inst2 specified in the configuration file, and executes itself again, now in stealth mode.
5. In this mode, the core component acts like a keylogger.
6. The core component (32-bit) executes the 64-bit version of itself, in injection mode (if applicable).
7. The core component (64-bit) injects the userland rootkit (64-bit) into task manager processes. The userland rootkit then hides presence of the malicious processes in the task manager.
8. The core component (32-bit) executes the RDS. It repeatedly monitors and hides the RDS window (because it is a GUI application).
9. The core component (32-bit) injects the userland rootkit (32-bit) into task manager processes. The userland rootkit then hides presence of the malicious processes in the task manager.
10. The core component (32-bit) executes commands cmd1 and cmd2, as specified in the configuration file. One of such commands was seen executing a GUI hider, which is an AutoHotKey script hiding the tray icon of the RDS.

Note: Some components are optional. Also, sometimes they are deployed as a set comprising an encrypted payload and the corresponding loader. We are omitting these details.

The configuration file of BalkanRAT is in INI file format (similarly to BalkanDoor, which uses this format for backdoor commands), with one section named [CFG]. The INI file is used by the malware' core component and the userland rootkit.

inst1, inst2	Commands executed by the core component during installation
cmd1, cmd2	Command executed by the core component main payload
hproc	List of processes that should be hidden by userland rootkit
mproc	List of processes where userland rootkit is injected



```
    stg_3.cfg                       ↓FRO --------           0      00000000|Hiew 8.43 (c)SEN
[CFG]
mproc=taskmgr.exe explorer.exe procexp.exe tasklist.exe
hproc=rfusclient.exe rutserv.exe winchk32.exe winchk64.exe wininit.exe weather.exe
cmd1=%appdata%/1B20F6AA-6CAD-45A7-81CB-120FB86FECD8/102/serk.bat
```

Figure 5. BalkanRAT's configuration file – properties (top) and example (below)

BalkanRAT's core is a multipurpose component (there are both a 32-bit and a 64-bit versions); it can be executed in various modes, determined by the command-line argument. Most significantly, it is used for installation of BalkanRAT, launching a userland rootkit and adding exceptions for the RDS component in the firewall.

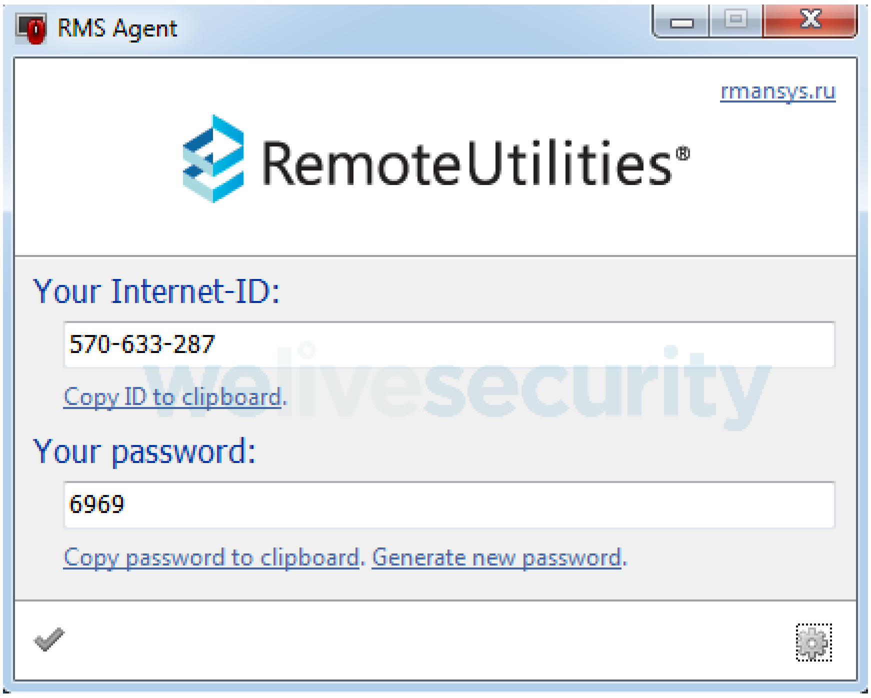
Argument	Functionality
/rhc	Executes a batch file
/fwl	Adds exception to the firewall for the specified program
/sreg	Sets configuration data for the RDS in the registry (especially email address where the credentials should be sent)
/inst	Ensures persistence by adding itself to the [HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows] registry key under the "load" entry. Adds exception for the RDS to the local firewall. Executes itself again in the main mode (no arguments).
/inj	Injects the userland rootkit library into processes, as specified in the configuration file
(none)	Main mode. Executes the 64-bit version of itself (if applicable), injects the userland rootkit, executes the RDS and hides the window by changing its coordinates to values outside the screen. Another thread captures pressed keystrokes.

The main part of the BalkanRAT malware is a copy of the Remote Utilities software for remote access. Instead of using the official version, BalkanRAT deploys a copy signed by a certificate of the attacker.

The client side of the RDS running on the victim's computer must know the unique ID and the password, both generated on the server side, to connect to the server. The RDS deployed by BalkanRAT is configured in such a way that the password is the same for all victims, and the generated unique ID is sent to the attacker's email address by the tool itself.

Since the tool BalkanRAT misuses is legitimate, it leverages the genuine Remote Utilities' infrastructure for this communication (rutils.com, server.rutils.com); due to this, the communication may seem legitimate to the user – and to security products.

As a result, the attacker has obtained credentials to access the compromised computer via the Remote Utilities software. Using this tool, they can broadcast the screen to monitor the activity of the user and manually take over the compromised computer.



Your Internet-ID:

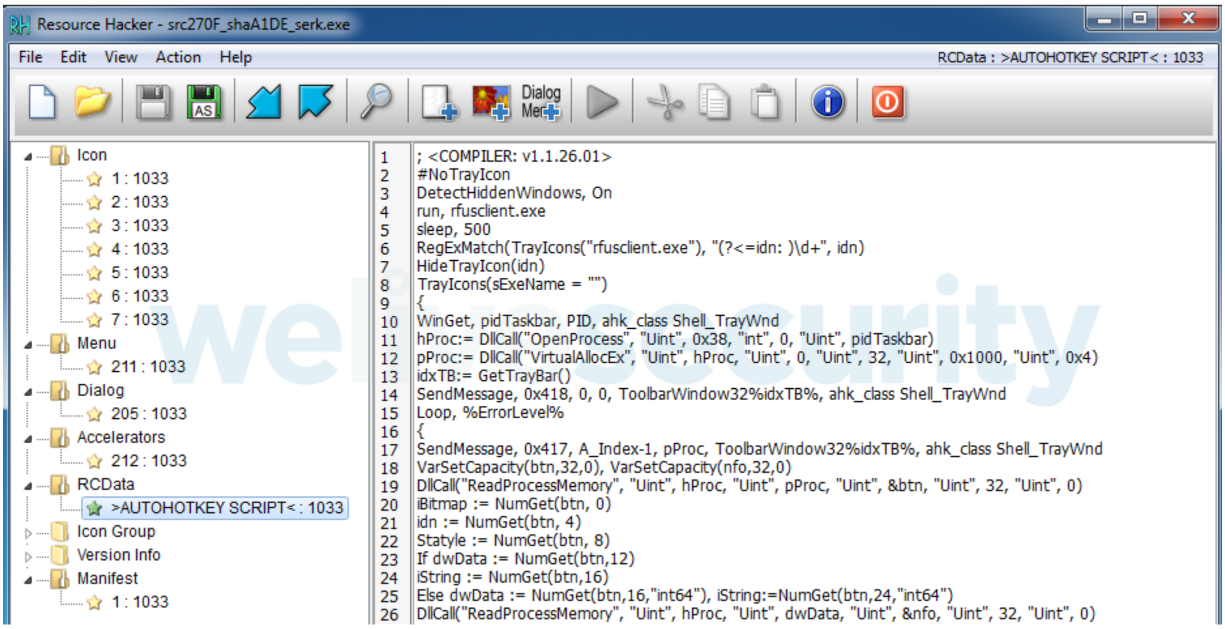
570-633-287

Your password:

6969

Figure 6. A window the victim never sees. With a legitimate copy of Remote Utilities, this window is visible; however, BalkanRAT will hide it using the GUI hider feature.

To remain stealthy, BalkanRAT uses the GUI hider feature. In most samples (some older ones are an exception), it is implemented as an AutoHotKey script, compiled into an executable file so that it can be run on a computer even if AutoHotKey is not installed there. The purpose of this script is to hide the tray icon of the RDS client.



```
; <COMPILER: v1.1.26.01>
#NoTrayIcon
DetectHiddenWindows, On
run, rfusclient.exe
sleep, 500
RegExMatch(TrayIcons("rfusclient.exe"), "(?<=idn: )\d+", idn)
HideTrayIcon(idn)
TrayIcons(sExeName = "")
{
WinGet, pidTaskbar, PID, ahk_class Shell_TrayWnd
hProc:= DllCall("OpenProcess", "Uint", 0x38, "int", 0, "Uint", pidTaskbar)
pProc:= DllCall("VirtualAllocEx", "Uint", hProc, "Uint", 0, "Uint", 32, "Uint", 0x1000, "Uint", 0x4)
idxTB:= GetTrayBar()
SendMessage, 0x418, 0, 0, ToolbarWindow32%idxTB%, ahk_class Shell_TrayWnd
Loop, %ErrorLevel%
{
SendMessage, 0x417, A_Index-1, pProc, ToolbarWindow32%idxTB%, ahk_class Shell_TrayWnd
VarSetCapacity(btn,32,0), VarSetCapacity(nfo,32,0)
DllCall("ReadProcessMemory", "Uint", hProc, "Uint", pProc, "Uint", &btn, "Uint", 32, "Uint", 0)
iBitmap := NumGet(btn, 0)
idn := NumGet(btn, 4)
Statyle := NumGet(btn, 8)
If dwData := NumGet(btn,12)
iString := NumGet(btn,16)
Else dwData := NumGet(btn,16,"int64"), iString:=NumGet(btn,24,"int64")
DllCall("ReadProcessMemory", "Uint", hProc, "Uint", dwData, "Uint", &nfo, "Uint", 32, "Uint", 0)
```

Figure 7. AutoHotKey script embedded in the resource section of the executable

Another notable feature used by BalkanRAT to stay hidden is the ability to hide processes from the user.

To achieve this, userland rootkit libraries are injected in processes hardcoded in the configuration file. The userland rootkit hooks the NtQuerySystemInformation function for the process in which it is injected. In case SystemProcessInformation is queried, it filters out all entries for processes with the names specified in the configuration file. As a result, conventional task manager utilities will not display the processes the attackers want to keep hidden from the user.

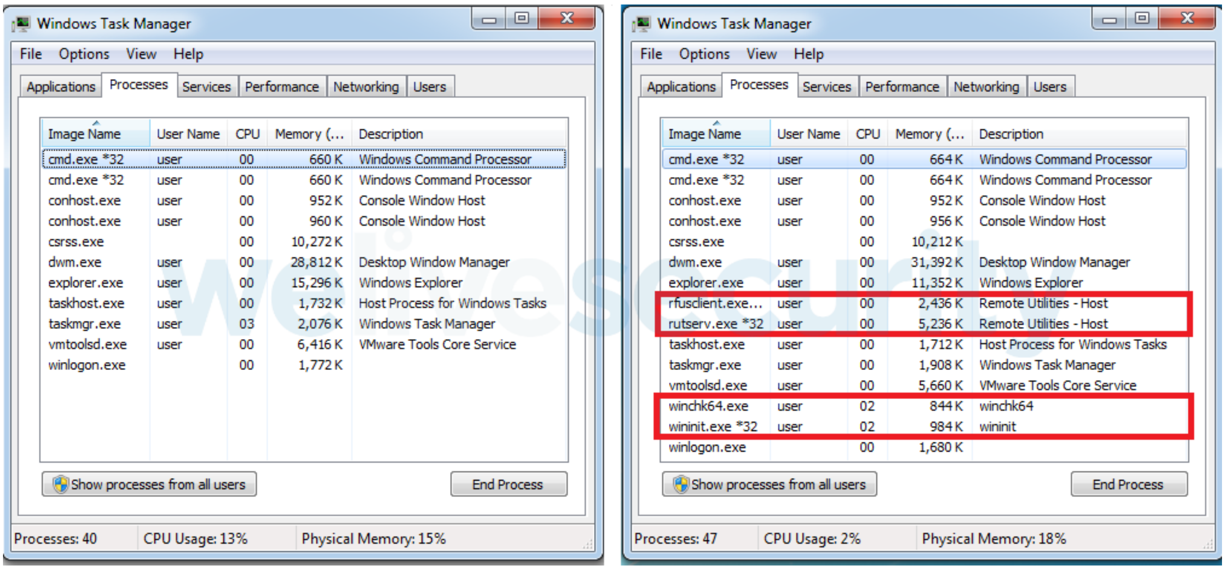


Image Name	User Name	CPU	Memory (...	Description
cmd.exe *32	user	00	660 K	Windows Command Processor
cmd.exe *32	user	00	660 K	Windows Command Processor
conhost.exe	user	00	952 K	Console Window Host
conhost.exe	user	00	960 K	Console Window Host
csrss.exe		00	10,272 K	
dwm.exe	user	00	28,812 K	Desktop Window Manager
explorer.exe	user	00	15,296 K	Windows Explorer
taskhost.exe	user	00	1,732 K	Host Process for Windows Tasks
taskmgr.exe	user	03	2,076 K	Windows Task Manager
vmtoolsd.exe	user	00	6,416 K	VMware Tools Core Service
winlogon.exe		00	1,772 K	

Processes: 40 CPU Usage: 13% Physical Memory: 15%

Image Name	User Name	CPU	Memory (...	Description
cmd.exe *32	user	00	664 K	Windows Command Processor
cmd.exe *32	user	00	664 K	Windows Command Processor
conhost.exe	user	00	952 K	Console Window Host
conhost.exe	user	00	956 K	Console Window Host
csrss.exe		00	10,212 K	
dwm.exe	user	00	31,392 K	Desktop Window Manager
explorer.exe	user	00	11,352 K	Windows Explorer
rfusclient.exe...	user	00	2,436 K	Remote Utilities - Host
rutserv.exe *32	user	00	5,236 K	Remote Utilities - Host
taskhost.exe	user	00	1,712 K	Host Process for Windows Tasks
taskmgr.exe	user	00	1,908 K	Windows Task Manager
vmtoolsd.exe	user	00	5,660 K	VMware Tools Core Service
winchk64.exe	user	02	844 K	winchk64
wininit.exe *32	user	02	984 K	wininit
winlogon.exe		00	1,680 K	

Processes: 47 CPU Usage: 2% Physical Memory: 18%

Figure 8. With the userland rootkit injected, some processes are missing in the list (left). Without the rootkit, the processes are visible (right).

Naturally, the list of processes that will be hidden contain mostly ones belonging to BalkanRAT. However, we have also seen names like “weather.exe” or “preserve.exe” in the list – which belong to the BalkanDoor backdoor. This finding supports the belief these two tools are indeed used together.

Conclusion

Both BalkanRAT and BalkanDoor have some interesting tricks up their sleeves and each of them separately pose a significant risk to the victims. If used together as a toolset, they make an even more powerful weapon – the more the campaign we have discovered targets accounting, a function that is critical for organizations.

The campaign targeting accountants in the Balkans shows some similarities with a campaign aimed at Ukrainian notaries reported in 2016. (The only source we have been able to find describing it is in Russian.) In that case, the attackers’ goal was to take control over a notary computer and issue some illegal operation on behalf of the notary.

Just as attackers may confirm a fraudulent transaction on behalf of a notary, they may perform a fraudulent transaction while impersonating a manager in a company’s financial department.

To stay safe, business users – and their employers – should follow basic cybersecurity rules: be cautious about emails and scrutinize their attachments and links, keep their software updated and use a reputable security solution.

Indicators of Compromise (IoCs)

ESET detection names

Win32/BalkanDoor.A
Win32/BalkanDoor.B
Win32/BalkanRAT.A
Win32/BalkanRAT.B
Win64/BalkanRAT.A
Win64/BalkanRAT.B

SHA-1

BalkanDoor – executable files

02225C58A0800A8FFFE82F7614695FDEEB75C8B3
3E8AF08F2C64D9D305A129FDEA6B24ED3D8D9484
400FF3FD5BEF94DCBEAE24B5B8A6632DCD1D22A6
576EF0057982DE87CA029C736706E840031A27F4
5CC4F248595268A0C9988DAEE3F0F8F9F5AC0A7F
60EB2A19EC63FF36D13F472EC0E6A594C2778CE6
7AA3D6EA4736C3BF627DB1837B9C8D2B29D7AB8D
AC5383306459CE8CD19BFF412875F093B40427C6

BalkanRAT – executable and auxiliary files

006B8EF615550BA731A30FA83B0E03CD16D2A92D
030DC8C3832F664FA10EFA3105DFF0A9B6D48911
032884A46430039ED4E38518AA20742B79AB2678
09D18CD045285A753BCF4F42C6F10AF76913546A
0F7A95C89911E3DE9205FF6AA03E1A4FCE6BC551
13D8664B438DA278CEB9C8593AE85023432054CD
17EA62EBC5F86997FD7E303FBBFF3E343DA38FCC
1C03ED1ADF4B4E786EFC00F3D892217FAAAFB268
15EC88015FB554302DB131258C8C11C9E46209D4
21DE3EB6F39DF4DBBF2D1FE4B6467AAE3D9FBEBD
21EE61874F299661AECC5453F4D6D0EC5380DAD0
270F1FA36365273F14D89EE852D8A438A594CD05
30BA2213BE4355D619E20DA733F27F59DA7B937E
3170B45FB642301687A3A320282099B9D7B7F0F2
38E7FCD6038E688DEC9F1AF9D2D222B9BBC03A8C
3927B48D315F6712D33166A3B278B7835E76A6A9
3C1FF7BBE8BC2BE9E5531FFAD25B18F03C51CF6B
421F52733D334BE32C899670426C06CB72D92CDE
46E4B456729CF659527D2697BD8518E67B5A0056
4F8BA64DA7EA16A7CE5AA2C83BBFCE1C8646E424
500A447A187240706C059C16366FEDF1AA13EA77
555844CA5CD40DFC27778C2D3B6AFA43D1B76685
5A3201048D8D9D696102A3C3B98DA99C2CC4FF1F
64E3A46BF393936A79478C891654C1070CEC42D1
685314454A7D7987B38ADD2EDDBAC3DB9E78464F
6C83ABE56219CA656B71AA8C109E0955061DA536
6E27F7C61230452555B52B39AB9F51D42C725BED
6EF16FAA19FC4CEF66C4C1B66E58FB9CFFD8098E

```
730E20EE7228080A7F90A238D9E65D55EDD84301
73E0A62F1AAAB3457D895B4B1E6E2119B8B8D167
7BA4D127C6CD6B5392870F0272C7045C9932DB17
7BF564891089377809D3F0C2C9E25FD087F5F42B
8852647B1C1A2EFA4F25FEA393D773F9FF94D6FA
8D9A804B1433A05216CFE1D4E61CE5EB092A3505
8F85738534158DB9C600A29B9DED8AC85C3DE8C1
963CF321740C4EF606FEC65FCE85FB3A9A6223AC
97926E2A7514D4078CF51EAC069A014309E607F1
9EA0C6A17EE4EB23371688972B7F4E6D4D53F3C8
9F2C6A44453E882098B17B66DE70C430C64C3B26
A1DEA762DD4329E77FE59526D4ABC0E15DE2BBBC
A56A299A8EEF9F4FF082184F66FAD1B76C7CACB8
A5ACE8F90C33CBDB12D398C0F227EC48F99551BF
AA4AD783DFE3CC6B0B9612814ED9418253203C50
AB311B53591C6625335B9B791676A44538B48821
AEDF43347AF24D266EC5D471723F4B30B4ACC0D0
B18222E93D25649BC1B67FAB4F9BF2B4C59D9A1A
B8F67BB5682B26ACD5969D9C6AC7B45FE07E79E1
BAD38D474D5CAAAC27082E6F727CAE269F64CF3C
BEEF0EE9397B01855C6DAA2BFF8002DB4899B121
BFE3F5CEC25181F1B6852E145013E548B920651E
C268CAB6D8EC267EEE463672809FAAEE99C2F446
C2F9FFDF518DA9E037F76902746DE89C2E2821E8
C3813734D3BFC07E339C05417055A1A106E2FBBD
C8CBBC175451A097E605E448F94C89D3E050ACD5
C90756A3C6F6DC34E12BABF5F26543510AACE704
C90B5471BBA3293C0A0E6829A81FBE2EB10B42B2
CD1BC431F53E9CFF8204279CDF274838DE8EBB61
CD82D898A3CEA623179456D9AE5FAD1FB5DA01A0
CDBB74CA0960F2E8631D49ACABF2CEA878AE35B8
CE7092FF909E9380CC647C3350AA3067E40C36A9
CEA70DB7FB8E851EF0D6A257A41C9CEE904345B5
CF7A8AFAC141E162A0204A49BAD0A49C259B5A45
DEEA26F5AF918CEC406B4F12184F0CAB2755B602
DFDFCC61770425A8D1520550C028D1DF2861E53F
E0007A2E0E9AE47DD028029C402D7D0A08EBBC25
E00C309E3FE09248B8AFCFF29FC1A79445C913DA
E95C651C539EAF73E142D1867A1A96098A5E219F
ECEEE01F4E8051F544062AE37D76A3DF2921DF82
F06CB000F9A25DDE791C7E5BC30917C74A8F2876
F26C663D5F6F534543A7C42B02254C98BB4EC0D5
F3BC2F436693B61FED7FA7DDF8BC7F27618F24F3
F6030AE46DC2CEF9C68DA1844F7DCEA4F25A90A3
FA19E71F9A836EA832B5D738D833C721D776781A
FFE23D510A24DB27C1C171D2BAF1FBEB18899039
```

Remote Utilities (otherwise legitimate releases signed by attackers' certificates)

038ECEB80597DE438D8194F8F57245EB0239FF4B
2A1BB4BB455D3238A01E121165603A9B58B4D09D
34CE3FBEE3C487F4F467B9E8EB36844BB5ACB465
3B88D4047FA2B8F8FA6241320D81508EB676EA7A
400438EB302886FD064274188647E6653E455EED
42F70DAA8C75E97551935D2370142C8904F5A20D
446D3FBAE9889FE59AFAD02C6FB71D8838C3FC67
4D46FB773C02A9FF98E998DA4F0777FB5D9F796B
510C93D3DC620B17500C10369585F4AF7CF3CE0D
6A5CA3B9EE0A048F0AEE1E99CBF3943D84F597FF
6D53E7B5099CE11ACA176519620E8064D4FF9AD0
7CEC39AC6A436577E02E7E8FE8226A00E58564CB
8888014C16732CD5136A8315127BA50BB8BB94ED
A5A05BA6E24226F1BC575CBC12B9FC59F6039312
B77CFFF0E359946029120DD642505BC0A9713ECC
BC6F31D5EBC71FF83BACC0B4471FDEFC206B28D0
BE8A582360FB16A4B515CD633227D6A002D142FA
C6E62A113E95705F9B612CDBF49DAC6BAD2073BD
D8D27C742DA87292EF19A197594193C2C5E5F845
DBE0E084B2A8CE4711C3DF4E62E8062234BF6D3B
E56189FE86C9537C28099518D4F4EA2E42EF9EEE
E918192D2B5C565A9B2756A1D01070C6608F361C

Scripts

0BD6C70B7E2320F42F0CFC2A79E161614C7C4F66
7A41B912A3F99370DF4CD3791C91467E23B2AA82
A15AB505B79B88A9E868C95CE544942403C58CB6
A8A5980DE35FBF580497B43EF7E8499E004F9F38
B248E43BAB127D8E1E466821B96B7B7ECF37CB78

Configuration files

28F152154F6E6074EA0DE34214102119C8589583
37A2A15C52CAA7D63AF86778C2DD1D2D81D4A270
B4A847D7AAC4164CF90EA585E4842CBF938B26CF

Decoy PDF files

1E0C4A5F0FF2E835D12C3B6571AE6000E81A014B
8722441FF3678D154C89E312DB1A54951DD21C3F
88C3FDA42768C5B465FD680591639F2CDC933283
9F48E109675CDB0A53400358C27853DB48FCD156
C9B592BD7B69995C75CD5B1E4261B229C27FB479

Misused certificates

AMO-K Limited Liability Company	llc.amo-k@list.ru	2015/07/30	2016/07/28	4E36C4D10F1E3D820058E4D451C4A7B77856BDB3	Expired
Valmpak, TOV	tov-valpak@mail.ru	2016/04/10	2017/04/01	17D50E2DBBAF5F8F60BFFE1B90F4DD52FDB44A09	Revoked
Valmpak, TOV	-	2016/08/22	2017/11/04	4A362020F1AFD3BD0C67F12F55A5754D2E70338C	Revoked
3D PEOPLE LIMITED	-	2017/11/05	2018/11/06	936EDFB338D458FBACB25FE557F26AA3E101506E	Expired
ADUNIK LTD	-	2017/10/11	2018/10/12	E7DF448539D1E2671DCF787CF368AAC2ED8F5698	Expired
SLOW BEER LTD	administrator@slowbeerltd.info	2019/01/25	2019/12/18	2359D644E48759F43993D34885167FECAFD40022	Revoked

File names

BalkanDoor

Dropper: Zakon.exe
Backdoors: weather.exe, winmihc.exe, Preserve.exe, PreservS.exe, WindowsConnect.exe
Scripts: weather.cmd, winmihc4.cmd, mihcupdate.cmd
Decoy PDF file: Zakon.pdf

BalkanRAT

Droppers: ZPDGI.exe, ZPDGV.exe, ZPDGE.exe, ZPDGO.exe, ZPDGU.exe, ZPDGA.exe, Ponovljeni-Stav.exe, AUG_1031.exe, MIP1023.exe
Configuration file: stg.cfg
Decoy PDF files: ZPDG.pdf, Ponovljeni-Stav.pdf, AUG_1031.pdf, MIP1023.pdf
Core component: winchk32.exe, wininit.exe, hide.exe, winchk64.exe
RDS: rutserv.exe, rfusclient.exe
Userland rootkit: winmmon.dll, winmmon64.dll
GUI hider components: serk.bat, serk.exe

Folder names

%WINDIR%\1B20F6AA-6CAD-45A7-81CB-120FB86FECD8
%WINDIR%\29D451CF-3548-4486-8465-A23029B8F6FA
%WINDIR%\B1EDD68E-6AD8-4A7E-91A1-3C30903B8DD4
%APPDATA%\1B20F6AA-6CAD-45A7-81CB-120FB86FECD8
%APPDATA%\29D451CF-3548-4486-8465-A23029B8F6FA
%APPDATA%\B1EDD68E-6AD8-4A7E-91A1-3C30903B8DD4

C&C servers

http://bestfriendsroot[.]com/smart.php
http://bestfriendsroot[.]com/weather.php
http://bestfriendsroot[.]com/zagreb.php
http://consaltingsolutionshere[.]com/smart.php
http://consaltingsolutionshere[.]com/weather.php
http://consaltingsolutionshere[.]com/zagreb.php
http://dogvipcare[.]net/kversion.php
http://hvar.dogvipcare[.]net/dekol.php
http://kimdotcomfriends[.]com/smart.php
http://kimdotcomfriends[.]com/weather.php
http://kimdotcomfriends[.]com/zagreb.php
http://limosinevipsalon[.]com/kversion.php
http://luxembourgprotections[.]com/kversion.php
http://malmevipbikes[.]se/kversion.php
http://split.malmevipbikes[.]se/dekol.php
http://zagreb.porezna-uprava[.]com/dekol.php

Email addresses used to exfiltrate Remote Utilities credentials

b.klokov@inbox.ru
galkin.valentin.83@bk.ru
gligorijmaskov@mail.ru
ivan.aslanov@newmail.ru
ivan.tatarov@qip.ru
melikov.viktor@yandex.ru
mr.aleksandrandreev@mail.ru
test@bbportal.info
tgerik@list.ru
vladzlobin@list.ru

MITRE ATT&CK techniques

BalkanRAT

Initial Access	T1192	Spearphishing Link	BalkanRAT is distributed via emails that contain links to malware.
Execution	T1059	Command-Line Interface	BalkanRAT uses cmd.exe to execute files.
	T1106	Execution through API	BalkanRAT uses ShellExecuteExW and LoadLibrary APIs to execute other malware components.
	T1064	Scripting	BalkanRAT uses batch scripts for malware installation and execution.

	T1204	User Execution	BalkanRAT relies on the victim to execute the initial infiltration. The malware is disguised as PDF documents with misleading names, in order to entice the intended victim to click on it.
Persistence	T1060	Registry Run Keys / Startup Folder	BalkanRAT uses the following Registry Run key to establish persistence: [HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows], “load”.
Privilege Escalation	T1134	Access Token Manipulation	BalkanRAT is able to impersonate the logged-on user using DuplicateTokenEx or ImpersonateLoggedOnUser APIs.
Defense Evasion	T1116	Code Signing	BalkanRAT is digitally signed with code-signing certificates.
	T1140	Deobfuscate/Decode Files or Information	BalkanRAT decrypts and decompresses some of its components.
	T1089	Disabling Security Tools	BalkanRAT is capable of adding exceptions to the local firewall, using its COM interface.
	T1112	Modify Registry	BalkanRAT modifies the [HKEY_CURRENT_USER\Software\Usoris\Remote Utilities\Server\Parameters] registry key to store configuration of the RDS
	T1027	Obfuscated Files or Information	Some components of BalkanRAT are compressed and then encrypted by a XOR cipher.
	T1055	Process Injection	BalkanRAT injects a userland rootkit library into processes of task manager utilities.
	T1108	Redundant Access	Operators of BalkanRAT have been seen deploying a second malicious tool (BalkanDoor) to preserve remote access in case BalkanRAT is removed.
	T1014	Rootkit	BalkanRAT uses a userland rootkit that hooks the NtQuerySystemInformation function to hide the presence of malicious processes.
	T1143	Hidden Window	BalkanRAT uses 3 rd party remote desktop software and hides its window and tray icon in order to hide it from the user.
Discovery	T1082	System Information Discovery	BalkanRAT collects the computer name and the language settings from the compromised machine.
Collection	T1056	Input Capture	BalkanRAT is capable of logging pressed keystrokes.
Command and Control	T1219	Remote Access Tools	BalkanRAT has misused legitimate remote desktop software for remote access.

BalkanDoor

Initial Access	T1192	Spearphishing Link	BalkanDoor is distributed via emails that contain links to download malware.
Execution	T1059	Command-Line Interface	BalkanRAT uses cmd.exe to create a remote shell.
	T1106	Execution through API	BalkanRAT uses ShellExecuteExW and LoadLibrary APIs to execute files.
	T1203	Exploitation for Client Execution	BalkanDoor can be distributed as an ACE archive disguised as a RAR archive, exploiting CVE-2018-20250 vulnerability in WinRAR to execute malicious code.
	T1064	Scripting	BalkanDoor uses batch scripts for malware installation and execution.
	T1035	Service Execution	BalkanDoor's backdoor can be executed as a service.
	T1204	User Execution	BalkanDoor relies on the victim to execute the initial infiltration. The malware is disguised as PDF documents or RAR archives with misleading names, in order to entice the intended victim to click on it.
Persistence	T1050	New Service	BalkanDoor can be installed as a new service, mimicking legitimate Windows services.
	T1060	Registry Run Keys / Startup Folder	BalkanDoor can be installed in the Registry Run key, or dropped in the Startup folder.
Privilege Escalation	T1134	Access Token Manipulation	BalkanDoor is able to create a process under the security context of a different user, using DuplicateTokenEx, SetTokenInformation or CreateProcessAsUserW APIs.
Defense Evasion	T1116	Code Signing	BalkanDoor is digitally signed with code-signing certificates.
	T1107	File Deletion	BalkanDoor deletes files with backdoor commands after the commands have been executed.
	T1158	Hidden Files and Directories	BalkanDoor sets attributes of its files to HIDDEN, SYSTEM and READONLY.
	T1036	Masquerading	BalkanDoor can be installed as a service with names mimicking legitimate Windows services.
	T1108	Redundant Access	Operators of BalkanDoor have been seen deploying a second malicious tool (BalkanRAT) to preserve remote access in case BalkanDoor is removed.
Discovery	T1082	System Information Discovery	BalkanDoor collects the computer name from the compromised machine.
Collection	T1113	Screen Capture	BalkanDoor can capture screenshots of the compromised machine.

Command and Control	T1043	Commonly Used Port	BalkanDoor uses ports 80 and 443 for C&C communication.
	T1090	Connection Proxy	BalkanDoor is capable of identifying a configured proxy server if one exists and then using it to make HTTP requests.
	T1008	Fallback Channels	BalkanDoor can communicate over multiple C&C hosts.
	T1071	Standard Application Layer Protocol	BalkanDoor uses HTTP or HTTPS for network communication.

Zuzana Hromcová 14 Aug 2019 - 11:30AM