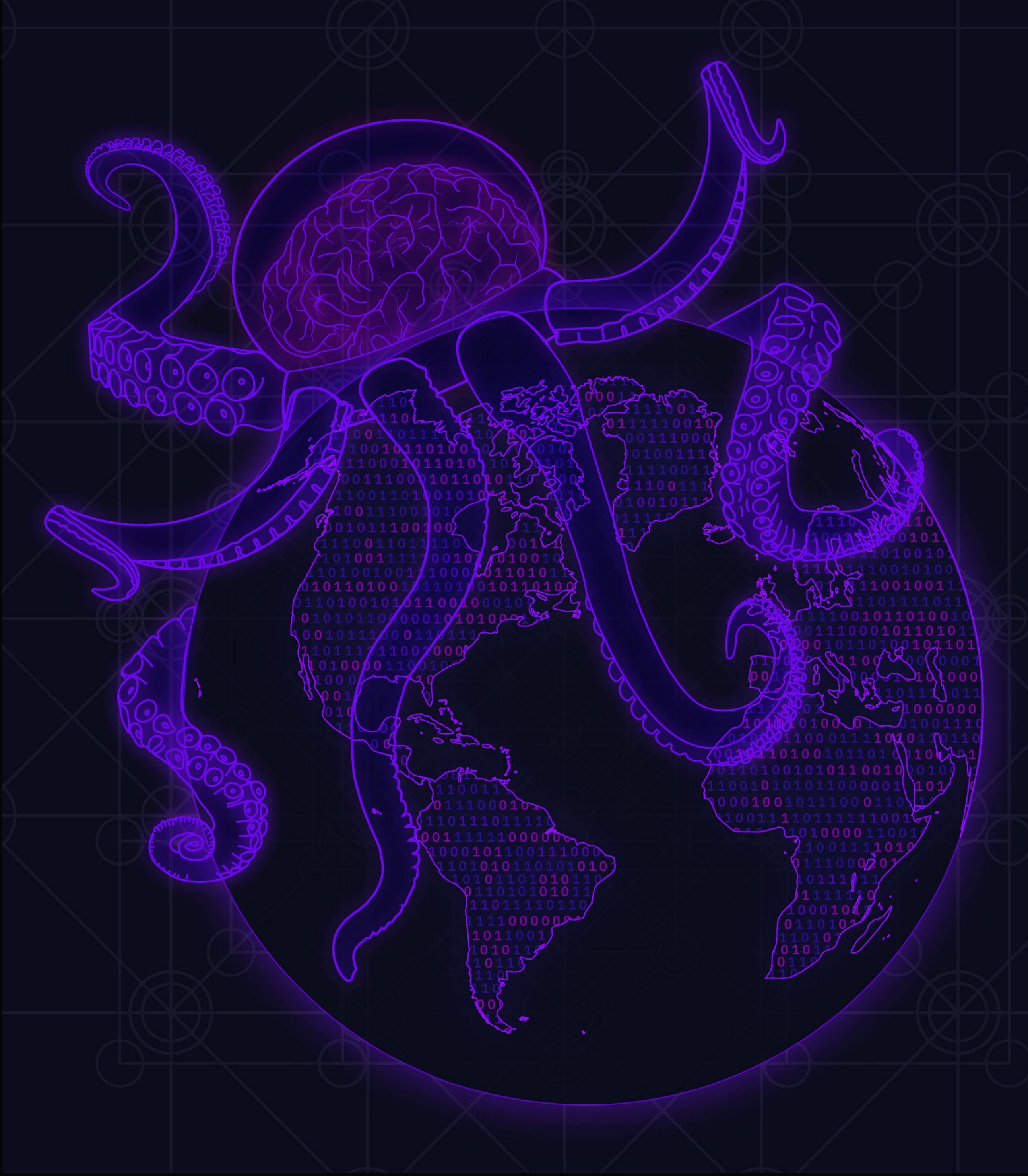


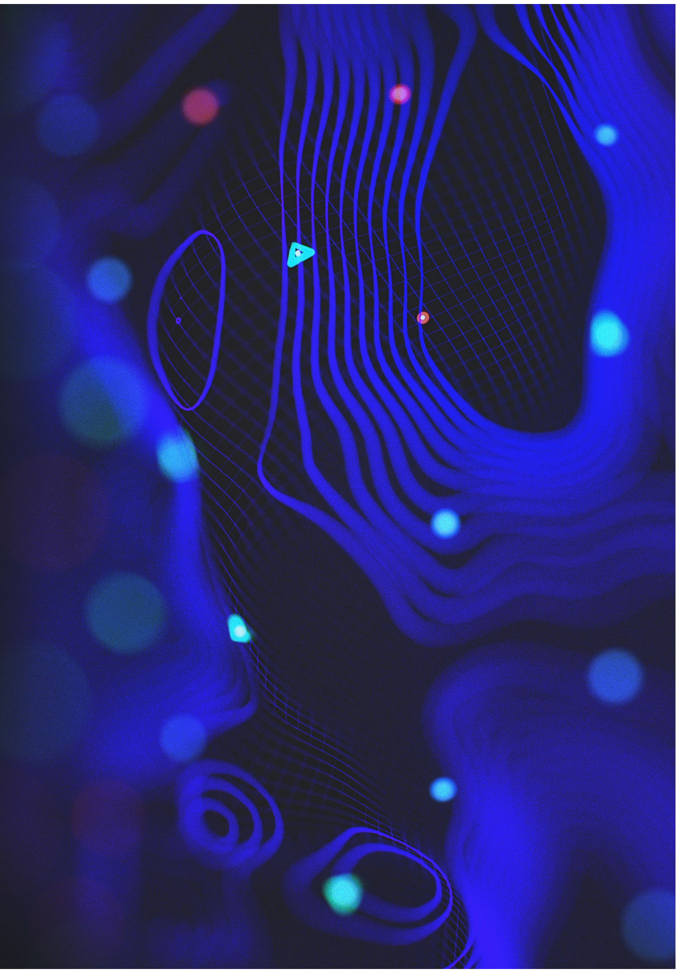
EGOMANIAC: AN UNSCRUPULOUS TURKISH-NEXUS THREAT ACTOR

Authors: Juan Andres Guerrero-Saade, Igor Tsemakhovich

September 2021

SentinelLABS Research Team

TABLE OF CONTENTS



EXECUTIVE SUMMARY

- This report sets the scope of a previously unknown threat actor we call ‘EGoManiac’.

- EGoManiac operated during the 2010-2016 timeframe, focusing primarily on Turkey and Turkish politics.

- EGoManiac is responsible for the previously reported ‘Octopus Brain’ campaign where the operators interdicted the machines of OdaTV journalists to place malware and incriminating documents, effectively framing them before arrest.

- Our research connects Octopus Brain to a toolkit called Rad, in development as early as 2010 and used until 2015.

- Rad samples use hardcoded email addresses for exfiltration.

- One of those email addresses is cited in connection to the prosecution of rogue members of the Turkish National Police along with executives of a company called ‘Datalink Analiz’. They refer to Rad as ‘HORTUM’.

- Following the trail of ‘Datalink Analiz’, we suspect that EGoManiac activity includes the use of HackingTeam’s Remote Control System (RCS) contracted under this same front company with a series of irregularities as early as 2011.

- In 2013, a report emerged on the use of RCS against a Turkish victim in the United States. The victim voiced an unverified suspicion that its use represented the unsanctioned interests of rogue Gülenist elements within the Turkish government.

SentinelLabs Team

THE HUNT FOR AHTAPOT

In the world of cyberespionage research, the human-interest element is often lost amidst a barrage of technical indicators. The absence of a human dimension can make our research seem overly technical and dry, something we write for defenders to block and other researchers to enjoy. When we can see the impact that some of these campaigns have on civil society and the weakening of public institutions, it invokes a certain doggedness that won't let sleeping dogs lie. 'EGoManiac' is one that's been in the back of our heads for the past five years. The research involved multiple dead ends, false starts, and layers of conspiratorial mystery.

What we refer to as EGoManiac is a cluster of two notable campaigns starting as early as 2010. The first campaign came to be known in research circles as 'Octopus Brain', based on the Turkish strings 'Ahtapot' and 'Bejin' left in the malware. This original campaign used a combination of publicly available RATs (including Turkojan and Bandook) as well as the closed-source Ahtapot, with delivery methods ranging from malicious documents to personal visits by the attackers.

Our initial awareness of this case came from Turkish court documents surrounding arrests of journalists at OdaTV. Much greater detail came to light thanks to the excellent work of the folks at Arsenal Consulting. Their forensic investigation not only proved the presence of the malware and the physical interdiction of the victim systems, but also established the attacker's access as the definitive source of the incriminating documents on those systems that were then used to justify arrests by the Turkish National Police. The journalists were ultimately acquitted by a court in 2017– six years after the attacks.

This scenario is one of the often-ignored dirty edge cases of 'lawful intercept' malware, stated plainly: what's the expectation of evidential integrity when it comes to an infected device?[1]

While these particular operators resorted to physically tampering with the devices they were monitoring, there's little keeping malware operators from placing incriminating or damaging files on systems infected with malware that has file download capabilities, as most rudimentary malware does.

In the face of such an unscrupulous actor, we are left to wonder if this activity is part of a cluster we already track, and if not, what else has this actor been up to in the shadows? Octopus Brain provided few answers. Despite finding a handful of Ahtapot modules, there were no newer samples nor connections to other toolkits. The trail went cold… until now.

[1] This question is currently playing out further in the Bhima Koregaon case in India, where it appears malware was used to upload incriminating letters onto the victim's machine– https://www.washingtonpost.com/world/asia_pacific/india-bhima-koregaon-activists-jailed/2021/02/10/8087f172-61e0-11eb-a177-7765f29a9524_story.html

EXPERIMENTS IN INNOVATIVE PIVOTING

As threat hunting technology continued to improve, there were different attempts to once again pick up the scent of the attackers behind the Octopus Brain campaign. Code similarity analysis is one of the favorite tools in our research arsenal. However, initial attempts to cluster new samples based on shared unique code snippets were not fruitful.

We decided to take a different approach. Rather than focusing on unique code snippets, we can instead focus on a bulk of shared common code as a way of profiling the development environment that produced the samples and attempt to find other samples produced in the same way– same compiler, same optimizations, relying on the same statically-linked libraries, etc. Limited testing of this method has yielded positive results under specific circumstances – like allowing us to cluster a set of samples based off of the analysis of a single original sample and without needing to spend cycles conducting extensive goodware testing.

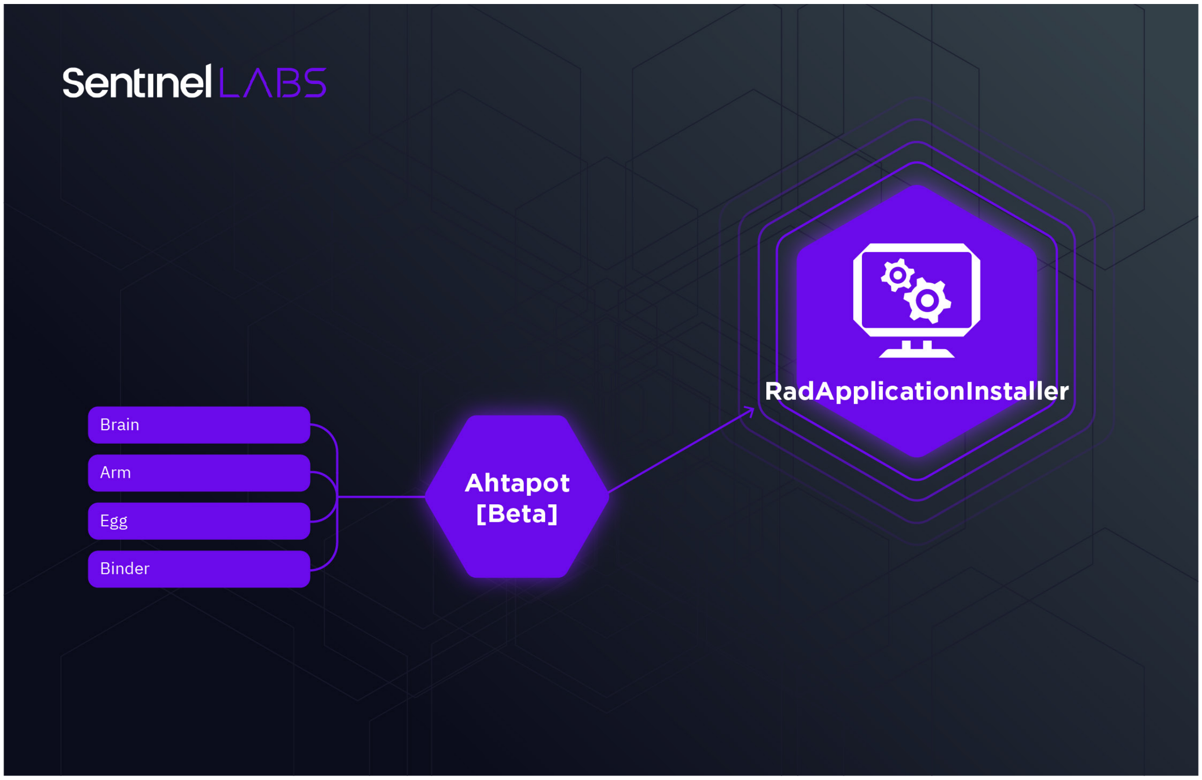
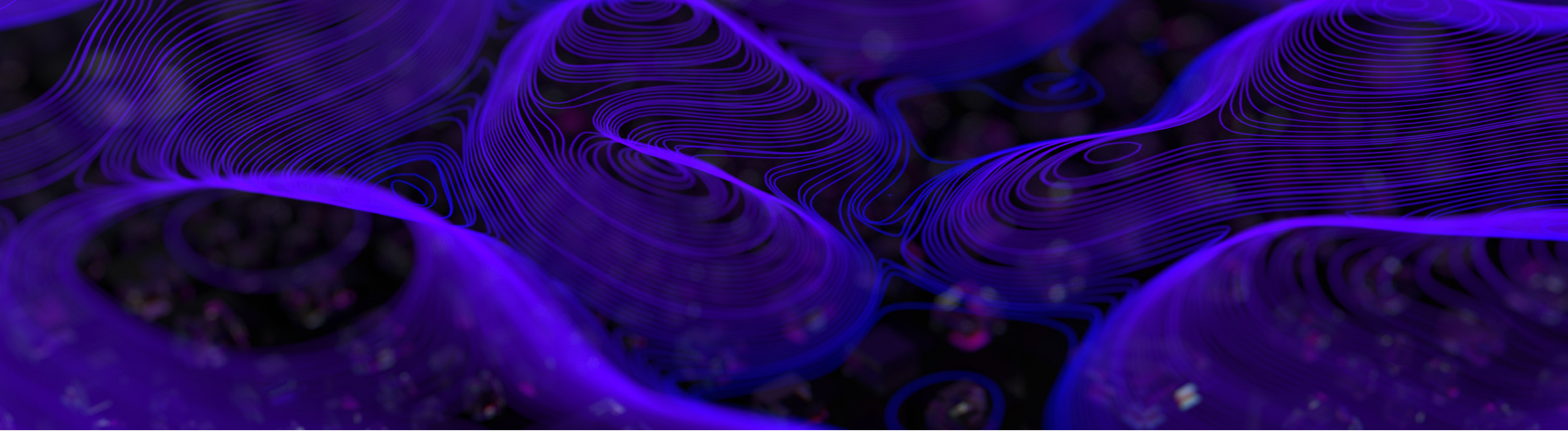
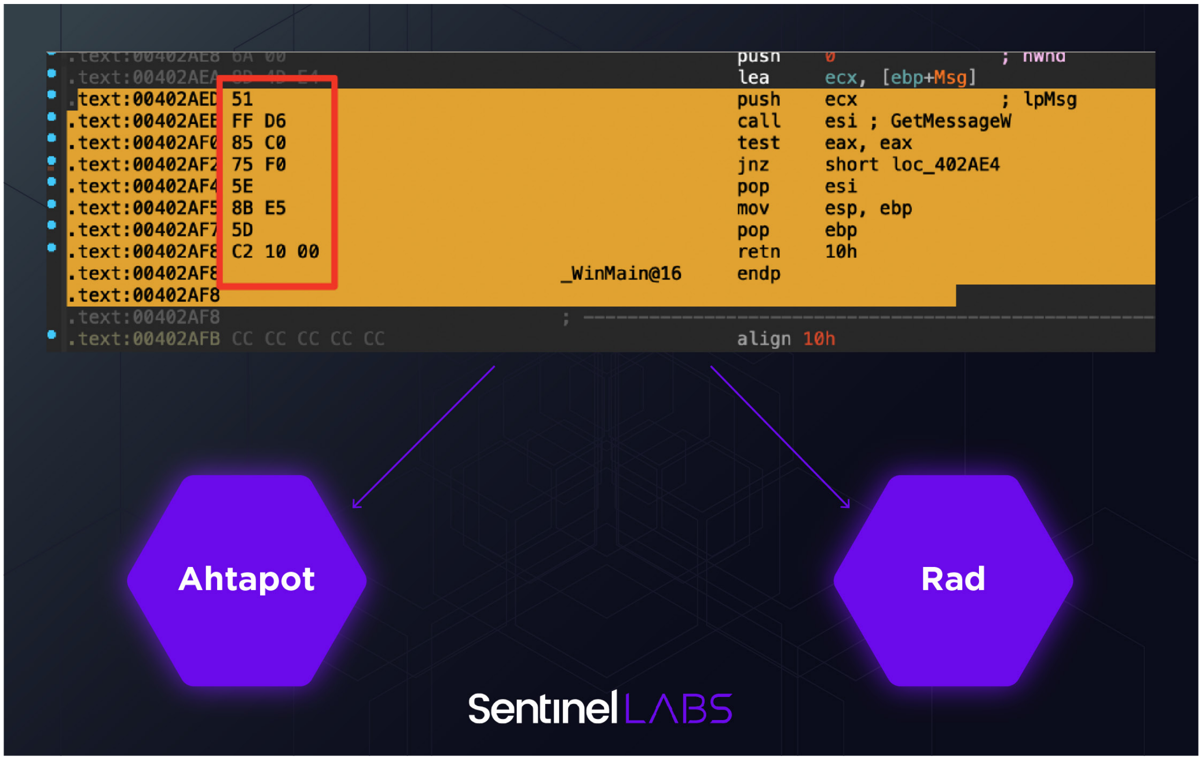


Fig 1: Ahtapot campaign components connect to newer Rad toolkit



To our surprise, applying this experimental approach to Octopus Brain yielded results. By generating a rule based off of the bulk of common code of Ahtapot components, we stumbled upon a set of samples we'll call 'Rad', based on a persistent typo in symbol paths left within the binaries.

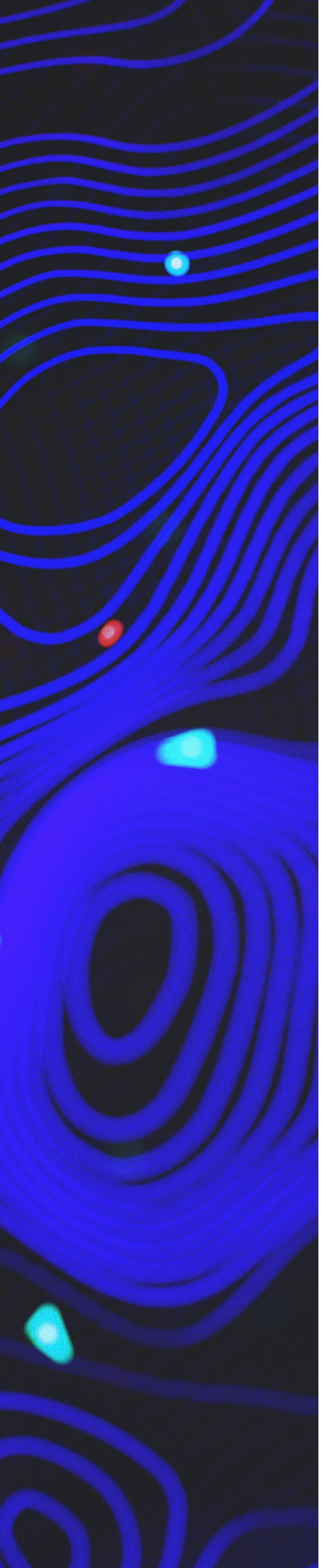
Expanding on this initial finding, we found a cluster of more than 50 samples and subcomponents for a modular espionage toolkit almost entirely undetected at the time of discovery.



```
.text:00402AE8 6A 00                                  push    0                   ; hWnd
.text:00402AEA 8D 4D E4                               lea     ecx, [ebp+Msg]
.text:00402AED 51                                     push    ecx                 ; lpMsg
.text:00402AEE FF D6                                  call    esi ; GetMessageW
.text:00402AF0 85 C0                                  test    eax, eax
.text:00402AF2 75 F0                                  jnz     short loc_402AE4
.text:00402AF4 5E                                     pop     esi
.text:00402AF5 8B E5                                  mov     esp, ebp
.text:00402AF7 5D                                     pop     ebp
.text:00402AF8 C2 10 00                               retn    10h
.text:00402AF8                         _WinMain@16    endp
.text:00402AF8
.text:00402AF8                         ; ---------------------------------------------
.text:00402AFB CC CC CC CC CC                         align 10h
```

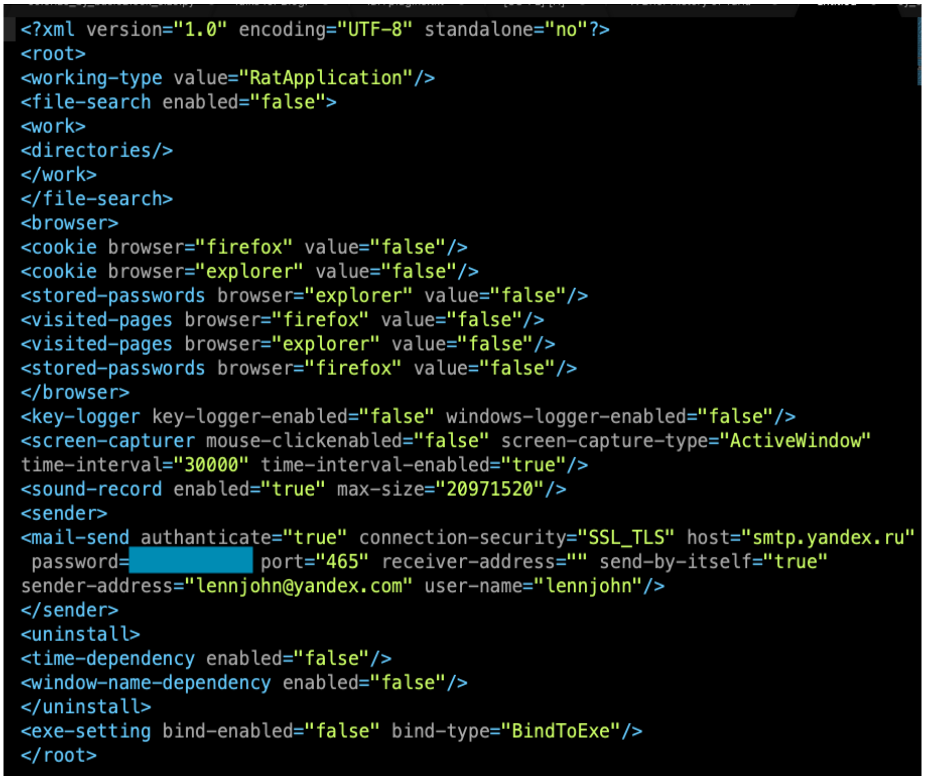
Fig 2: Unique code segment connecting Ahtapot and Rad campaigns

Our friends at Kaspersky's GReAT were able to blind confirm our finding using their KTAE attribution engine, honing in on a unique code segment shared by the first-stage components of both Ahtapot and Rad.



EGOMANIAC’S ‘RAD’ TOOLKIT

Rad is a modular espionage malware toolkit built around the POCO C++ cross-platform development libraries. The design entails a form of organized development but not a particularly savvy or sophisticated one at that. POCO is doing most of the heavy lifting. Functionality is split into modules contained within a ‘RadApplicationInstaller’ and orchestrated by a ‘RadStarter’ module that takes its cues from an encrypted configuration XML file.



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<root>
<working-type value="RatApplication"/>
<file-search enabled="false">
<work>
<directories/>
</work>
</file-search>
<browser>
<cookie browser="firefox" value="false"/>
<cookie browser="explorer" value="false"/>
<stored-passwords browser="explorer" value="false"/>
<visited-pages browser="firefox" value="false"/>
<visited-pages browser="explorer" value="false"/>
<stored-passwords browser="firefox" value="false"/>
</browser>
<key-logger key-logger-enabled="false" windows-logger-enabled="false"/>
<screen-capturer mouse-clickenabled="false" screen-capture-type="ActiveWindow"
time-interval="30000" time-interval-enabled="true"/>
<sound-record enabled="true" max-size="20971520"/>
<sender>
<mail-send authanticate="true" connection-security="SSL_TLS" host="smtp.yandex.ru"
 password=[redacted] port="465" receiver-address="" send-by-itself="true"
sender-address="lennjohn@yandex.com" user-name="lennjohn"/>
</sender>
<uninstall>
<time-dependency enabled="false"/>
<window-name-dependency enabled="false"/>
</uninstall>
<exe-setting bind-enabled="false" bind-type="BindToExe"/>
</root>
```

Fig 3: Extracted Rad configuration XML
(92abdfa8d72cd42f6e6f3ad903380df5397e6ea8328c47422f8e016ee204f3bc)

The XML tells Rad which modules to switch on or off, specific configurations like the time intervals for screen captures and max filesize for sound recordings, and most importantly – what email to use for exfiltration. All of the Rad samples we’ve found rely on email exfiltration with a hardcoded address belonging to either Gmail, Yandex, or Woxmail (defunct at the time of writing). This style of exfiltration entails both pros and cons for the attackers.

Pros:

- Email traffic is unlikely to be blocked or considered suspicious in the target environment
- There's no obvious infrastructure for defenders to track, pivot on, or sinkhole for victim data

Cons:

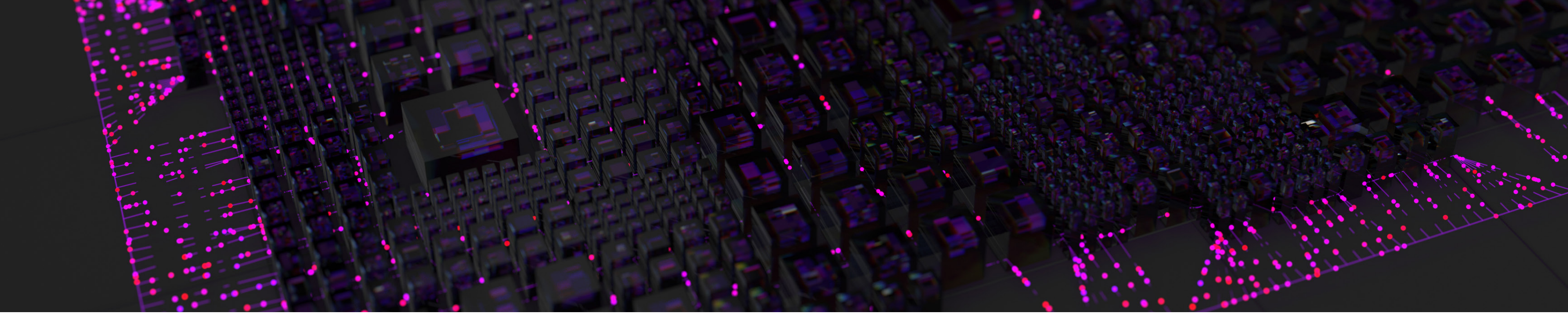
- Exfiltrated data is subject to size limitations
- Exfiltrated data is available to the hosting providers as well as anyone able to reverse engineer the malware configuration[2]

The more bizarre angle of the malware's functionality is its lack of command-and-control capabilities. The malware will follow its original configuration without recourse to additional commands, updates, or changes. This is perhaps the most unusual aspect of the malware.

Exfiltration via email is unlikely to be favored by an experienced group operating on the world stage. It's perhaps more acceptable to mercenaries or a regionally focused threat group. In this case, rather than cause another research dead-end, one of those email addresses might provide the greatest attribution connection of all, more on that later.[3]

[2] It's worth noting that the attackers obfuscated the exfiltrated data to provide some level of protection against third-party prying eyes and fourth-party collection.

[3] See §A Wilderness of Mirrors.



TOOLKIT STRUCTURE

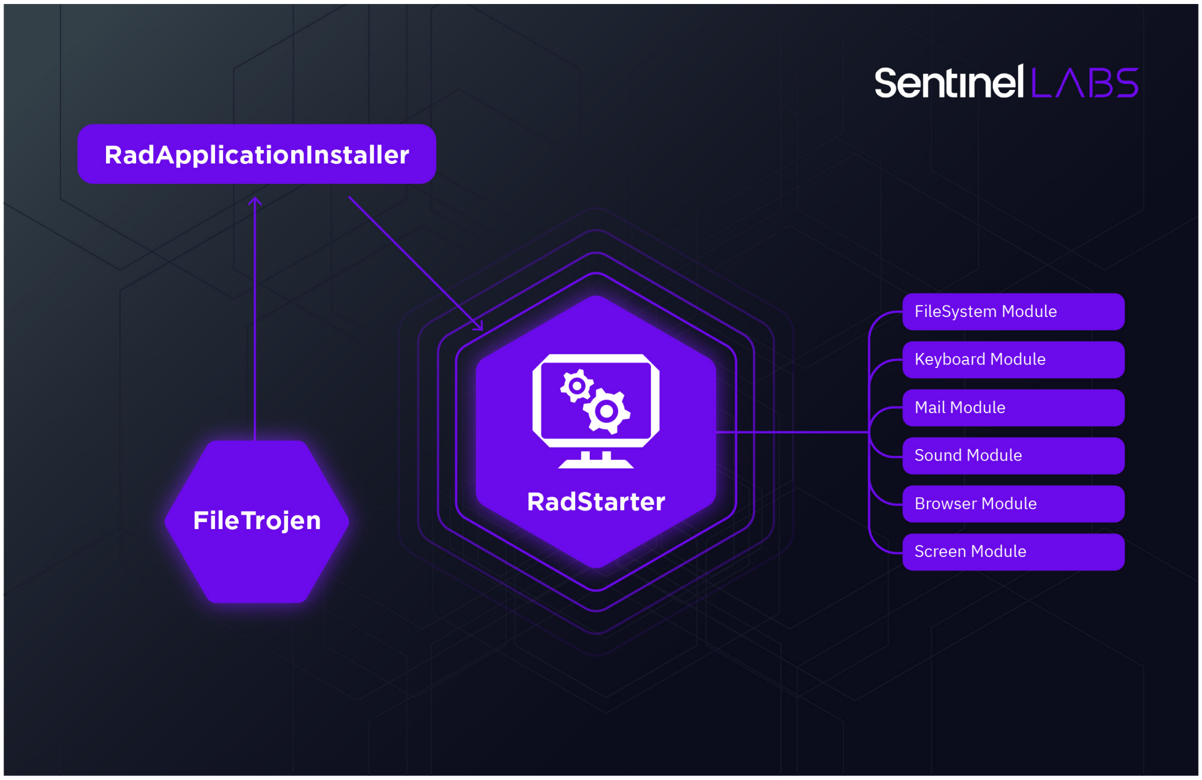
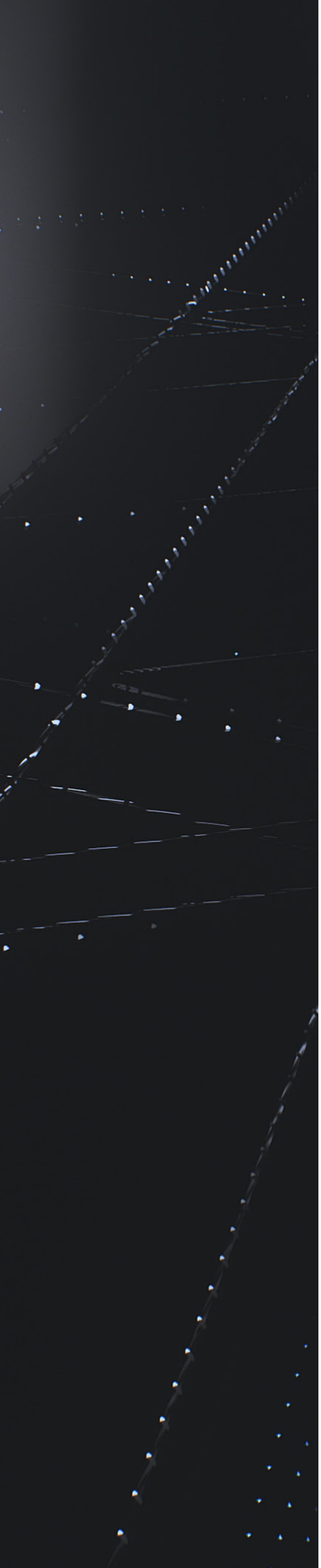


Fig 4

The execution flow of the Rad toolkit is straightforward. ‘wsms.exe’ (RadStarter) is the main module that runs from a registry key set by the installer. It, in turn, runs the other modules as separate processes. These include:

Internal Name	Process Name	Functionality
RadStarter	wsms.exe	Main orchestrator
RatKeyboardModule	SynTPHelper.exe	Keylogger
RatSoundModule	VolCtrl.exe	Hot mic recorder
RatBrowserModule	AtService.exe	Browser information extractor
RatScreenModule	QLBCtrl.exe	Screen-capture module
RatMailModule	SearchIndexer.exe	Communication module
RatFileSystemModule	WmiPrvSE.exe	File enumeration and search



The main package also includes the POCO dependency DLLs used by the modules:

- PocoFoundation.dll is the core dependency
- PocoCrypto.dll wraps OpenSSL library APIs
- PocoXML.dll provides XML parsing primitives
- PocoNet.dll and PocoNetSSL.dll are communication libraries based on socket and SSL APIs, respectively.

This is not the first malware family developed using the POCO C++ libraries. Russian APTs have relied on POCO in the past, including a downloader associated with APT28 ('PocoDown') and the fabled Drovorub.

DEVELOPMENT NOTES

The modules' internal names are derived from PDB paths consistently left within the binaries, allowing for an appreciation of the developers' organizational skills and lack of regard for operational security. This sets the general tone for Rad's development consisting of straightforward method implementations around standard APIs. Screen capture relies on GDI APIs, keylogging is done via GetAsyncKeyState, and sound recording is done via a multimedia library. Binaries are not obfuscated and export names are in plaintext.

Charitably, the developers may have intended to avoid arousing the suspicion of anti-malware software by doing everything in a documented and innocent looking way devoid of evasion. Low detection numbers at the time of discovery support the value of this approach. However, the loud multi-process structure of the malware and absence of checks for security software on target systems suggest the developers are simply inexperienced in the world of malware development.

Further supporting the general timeline of the Rad campaign, development of the main Rad components was carried out using Visual Studio 2010 and dependency DLLs built in 2012. As with all compilation timestamps, it's possible that these were altered.

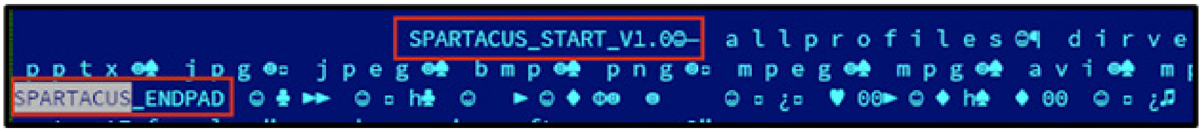
INFECTION VECTORS

We were only able to recover a small subset of infection vectors utilized by EGoManiac to place the Rad malware on target systems. In one case, we see an email[4] in Turkish pretending to be from a local telecommunications provider:

Değerli Abonemiz ; Siz değerli üyelerimize daha iyi hizmet vermek için çalışıyoruz. Sistemlerimizde kayıtlı müşterilerimiz için çeşitli hediye paketleri oluşturduk. Size özel hazırlanmış hediye içeriğini görmek için ekteki dosyayı inceleyiniz. Saygılar TURKCELL	Dear Subscriber; We are working to serve you, our valuable members, better. We have created various gift packages for our customers registered in our systems. Please check the attached file to see the gift content prepared for you. Regards TURKCELL
Original	English

The email contains a zip archive[5] with the executable 'Turkcell_hediye.exe'[6], roughly translated to 'Turkcell Gift'. The executable is a straightforward RadApplicationInstaller package meant to infect the victim with no attempt at displaying a lure or feigning benign functionality for the user.

Additional early-stage droppers include a RAR archive named 'gercekler.rar'[7] (containing an executable of the same name), as well as a variant that actually displays a lure for the victim (internally referred to as FileTrojen). The lure is a Turkish PowerPoint presentation on the development of management skills. The malware is connected to EGoManiac via a consistent PDB path convention. FileTrojen appears to be an earlier version of the Rad FileSystemModule built before the adoption of the POCO C++ libraries. It includes functionality for tracking USB keys connected to victim systems and their contents.



```
                              SPARTACUS_START_V1.0   a l l p r o f i l e s   d i r v e
p p t x   j p g   j p e g   b m p   p n g   m p e g   m p g   a v i   m
SPARTACUS_ENDPAD
```

Fig 5: FileTrojen configuration headers

Interestingly, the configuration for this variant is encapsulated within the tags 'SPARTACUS_START_V1.0' and 'SPARTACUS_END' perhaps suggesting its internal naming convention.

[4] 5e02f7d0337750be8dd36c96638b8f44127d6fdabe5d7ae04b11fd3ca2d14de4, Turkcell Müşteri Hizmetleri.eml

[5] dd60b8f2144de64ed1e2182d511d68ca0c60e1de0d8fa4a6bf80c9701c0ced52, turkcell_hediye.zip

[6] 3d3f208e54da010a571bc53296621428786cecb624f4c433d83dd4f40908820c, turkcell_hediye.exe

[7] 4cbb8e0bde66af241819c7492db0a9084b9c504dc3f69b7d8e5ef77198008991, gercekler.rar

WHO IS EGOMANIAC?

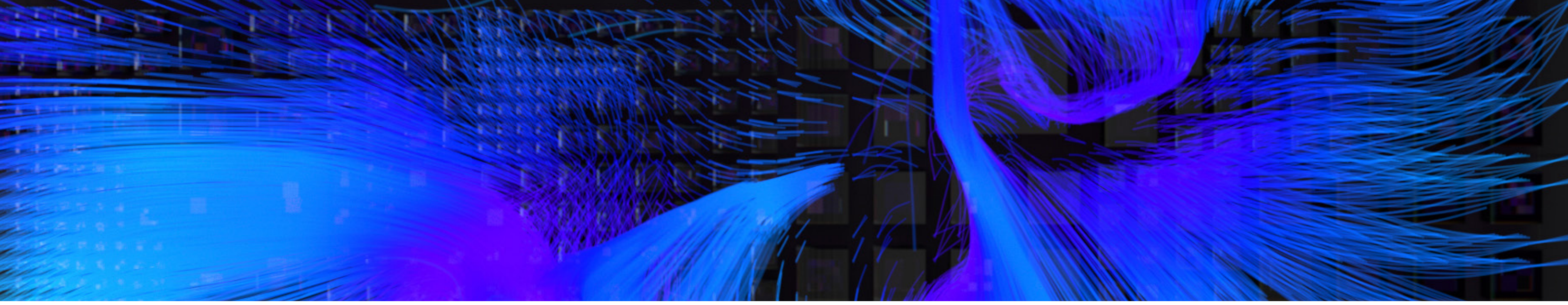
Attribution based solely on technical indicators is complicated and inexact. Most technical indicators are subject to modification and require interpretation based on limited visibility. Lacking a greater understanding of local context and closed-source intelligence, it's difficult to extend attribution beyond abstract entities (like an APT group name) to specific people or organizations.

On the surface, EGoManiac activity revolves around a Turkish nexus. Malware is riddled with Turkish language, lures are written in Turkish, victims are Turkish and relevant to local politics. The connection to Ahtapot and the OdaTV incident entails the actor's ability to physically interdict systems within Turkey. Additionally, most PDB paths for Rad components have a root folder of 'EGM', from which we derived the name 'EGoManiac'.

Three samples deviate from this PDB naming convention to use a root folder of 'SEA'[8], a reference to the Syrian Electronic Army. This association is further reinforced by the inclusion of throwaway strings like 'Syrian Electronic Army', 'sea.sy', and 'Codename Assad' in the binaries. The compilation timestamp maps onto the emergence of the Syrian Electronic Army in late 2011. This is likely an early attempt at misdirection and is not sustained in any of the later samples.

As we dig deeper into this Turkish nexus, the attribution angle only gets more complicated.

[8] bcd5e2ac31b250e665691487f8eda0d2d170a4f31fad0aba158f73445351654f,
0a9357e9db888a601ade886fb54fa4eacdcfee72e3145dfbb26ae9492abfd877,
3d3f208e54da010a571bc53296621428786cecb624f4c433d83dd4f40908820c.



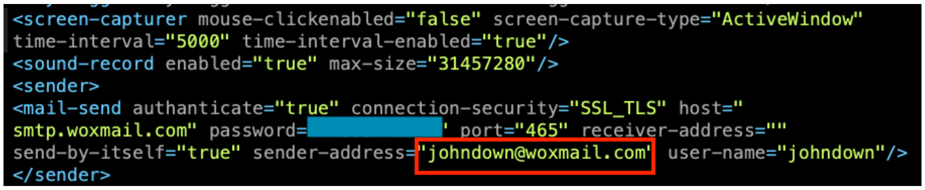
A WILDERNESS OF MIRRORS

EGoManiac's Rad toolkit relies on hardcoded email addresses for communication. Obfuscated logs and other exfiltrated materials are sent to the following emails across multiple service providers:

While email comms might usually lead to another research dead-end, the address 'johndown@woxmail.com' raised an interesting connection.

In 2016, Turkish websites reported sparse details of an ongoing attempt to prosecute members of the Turkish national police and executives of an IT company called 'Datalink' suspected of leaking information on active police operations. The leaks were reportedly used by FETO/Gülenist movement social media accounts to fuel conspiratorial elements in an ongoing power struggle within the country.

Reports cite the use of spyware called 'HORTUM' (roughly translated as 'garden hose') to siphon data from infected machines within public institutions in Turkey including the Intelligence department of the General Directorate of Security (EGM). Some of the reporting mistakenly conflates HORTUM with HackingTeam's RCS. The siphoned data was sent to 'johndown@woxmail.com' and from there allegedly redistributed by Datalink. The capabilities of HORTUM and its communication methods match those of EGoManiac's Rad, including the hardcoded Woxmail address.



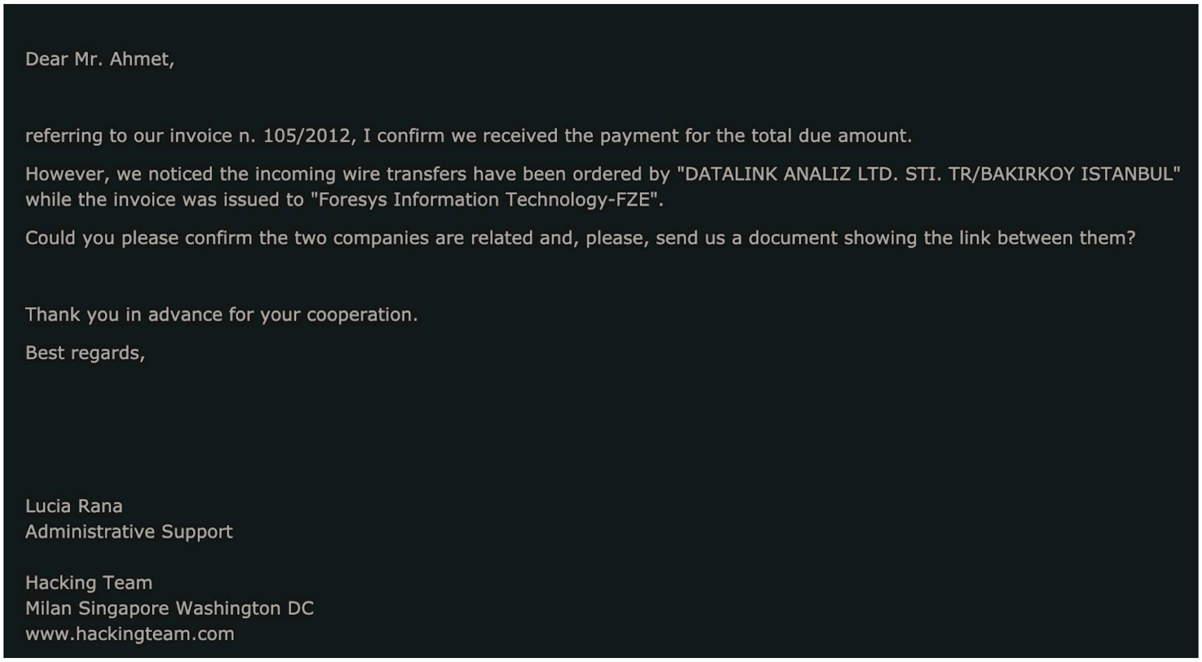
```
<screen-capturer mouse-clickenabled="false" screen-capture-type="ActiveWindow"
time-interval="5000" time-interval-enabled="true"/>
<sound-record enabled="true" max-size="31457280"/>
<sender>
<mail-send authanticate="true" connection-security="SSL_TLS" host="
smtp.woxmail.com" password=[redacted]' port="465" receiver-address=""
send-by-itself="true" sender-address="johndown@woxmail.com' user-name="johndown"/>
</sender>
```

Fig 6: Encrypted configuration using johndown@woxmail for exfiltration (b79df7817ac1f39692927a593bf0569fd57e3faaebbbf4a0c7b452e7928157cb)

We cannot independently verify the veracity of the initial reporting. An independent investigation to that effect was conducted by Kim Zetter, who obtained extensive details including a report by the prosecutor handling the case. Taking the information we have at face value, we uncover another possible facet of the EGoManiac story.

THE HACKING TEAM CONNECTION

As early as 2012, victims of HackingTeam's Remote Control System (RCS) 'Da Vinci' began to show up in Turkey. In 2013, Wired reported that a woman in the United States was targeted with RCS. The victim suspected that she was targeted by Gülenist elements that had infiltrated the Turkish government. However, HackingTeam continued to assert that it only sells its tools to governments and did not confirm Turkey's status as a customer. Now, in the aftermath of Phineas Fisher's devastating hack-and-leak operation against HackingTeam, we can independently confirm that Turkey was in fact a customer of HackingTeam at the time –but who exactly was their customer in Turkey?



Dear Mr. Ahmet,

referring to our invoice n. 105/2012, I confirm we received the payment for the total due amount.

However, we noticed the incoming wire transfers have been ordered by "DATALINK ANALIZ LTD. STI. TR/BAKIRKOY ISTANBUL" while the invoice was issued to "Foresys Information Technology-FZE".

Could you please confirm the two companies are related and, please, send us a document showing the link between them?

Thank you in advance for your cooperation.

Best regards,

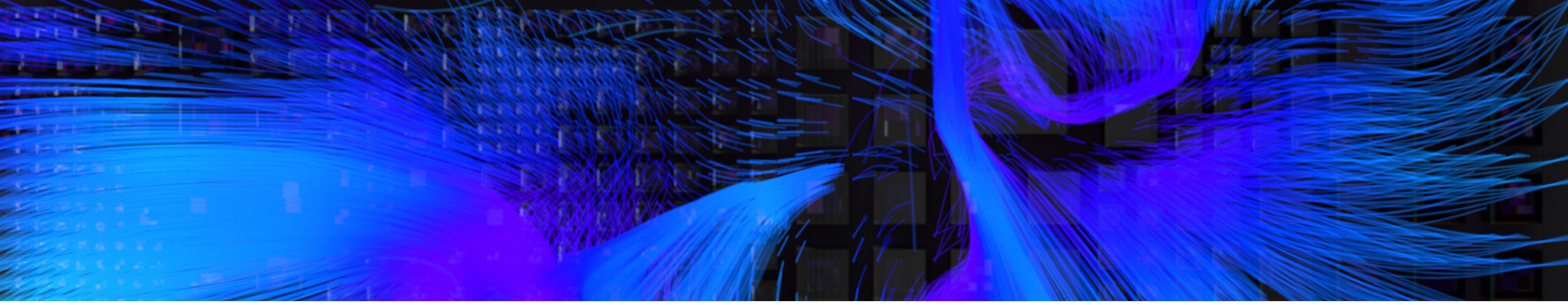
Lucia Rana
Administrative Support

Hacking Team
Milan Singapore Washington DC
www.hackingteam.com

Fig 7: Leaked HackingTeam email on an invoice confusion involving an Istanbul company 'Datalink Analiz'

The leaked HackingTeam treasure trove contains communications with officials claiming to be a part of the Turkish National Police as early as 2011. Citing problems with their mail server, they proceed to use three Gmail accounts[9] to plan their purchase of RCS. A Gmail account is also used for communication with the HackingTeam support portal. HackingTeam officials note further irregularities as the first deal goes through. Though the purchase is intended under the umbrella of a UAE-based shell company ('Foresys Information Technology-FZE'), HackingTeam receives payment from a company registered in Istanbul– 'Datalink Analiz LTD'.

[9] tnp.notcenter@gmail.com, tnpnotcenter2@gmail.com, akocak005@gmail.com



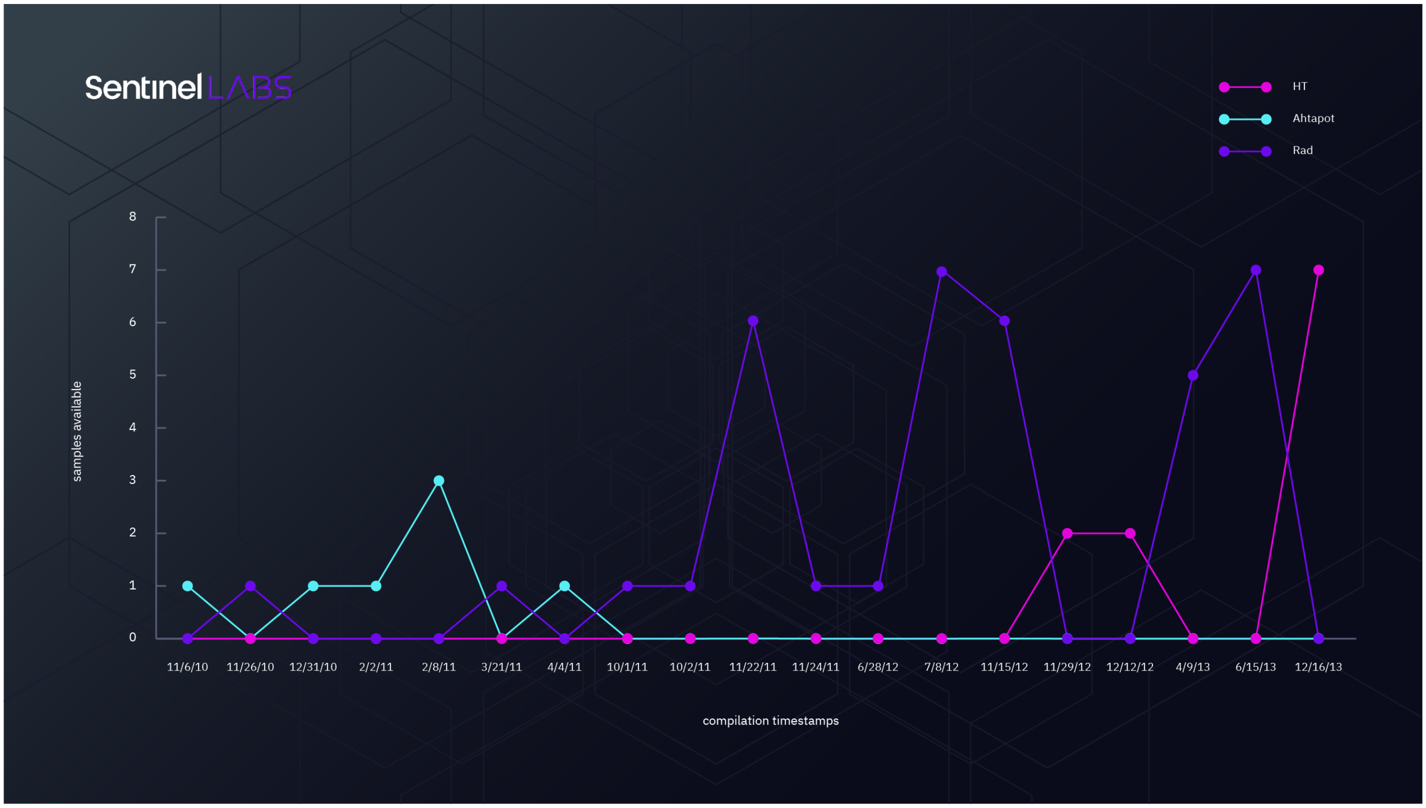
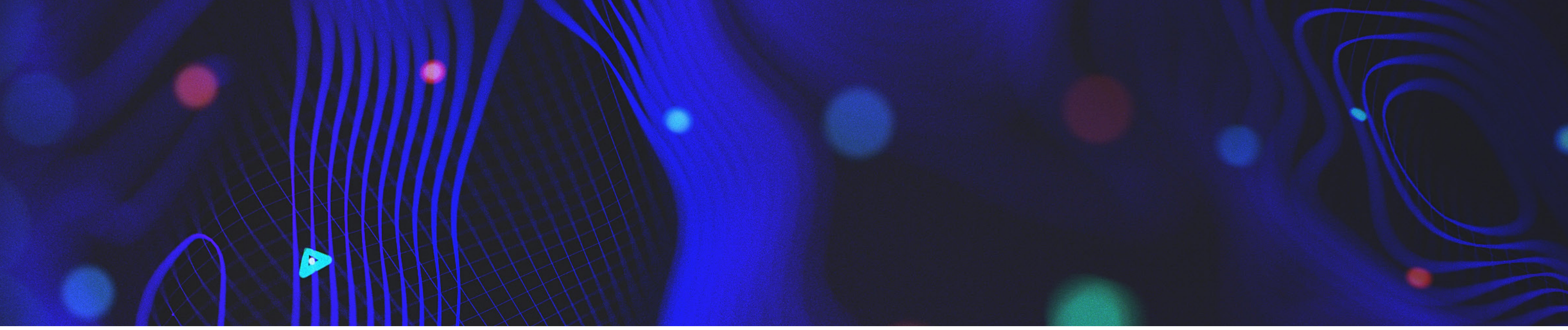


Fig 8: Revalence of EGoManiac-related malware families by compilation timestamp

To be thorough, we chart the use of Hacking Team RCS by the Turkish National Police (Appendix C) based on the company's internal watermarking scheme used to track the origin of leaked samples among their customer base. The graphic above notes the coincidental cadence of the use of the different malware families related to the EGoManiac cluster. However, we can't go as far as to equate the two clusters without resolving the murky allegiances of the operators involved.

The connection between the EGoManiac umbrella and this specific sub-cluster of Hacking Team RCS is built on the admittedly thin strand of the 'Datalink Analiz' shell company. That thread merits an investigation beyond the purely technical to straighten out an abundance of conspiratorial claims, alleged foreign money laundering, and ambiguous finger pointing.



CONCLUSION

The case of EGoManiac is far from straightforward. It involves difficult investigative connections that test the boundaries of our visibility, the efficacy of our research tools, and the limits of purely technical attribution. Beyond the technical exercise, it's a profile of a threat actor willing to spy on both friend and foe and to use that access to malign and entrap journalists without compunction. While this particular intrusion set is outdated, the questions it raises speak to the friction between the unsupervised governmental use of malware and the integrity of public institutions, rule of law, and evidentiary standards. They are more relevant now than ever before.

REFERENCES

1: https://www.vice.com/en/article/nz74wq/turkish-journalist-jailed-for-terrorism-was-framed-forensic-report-shows-1

2: https://arsenalexperts.com/Case-Studies/Odatv/

3: https://www.vice.com/en/article/ezpkjz/some-malware-victims-in-turkey-have-no-idea-theyve-been-targeted

4: https://securelist.com/spyware-hackingteam/37064/

5: https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

6: https://www.wired.com/2013/06/spy-tool-sold-to-governments/

7: https://www.dailydot.com/debug/hacking-team-turkey/

8: https://www.karar.com/emniyete-paralel-casus-hortumu-142749

9: https://www.karar.com/paralel-sizinti-casus-hortumdan-146792

10: http://www.ayorum.com/haber_oku.asp?haber=4245

TECHNICAL APPENDIX A: AHTAPOT (2010-2011)

PDBs

```
E:\Projeler\Ahtapot\Release\Ahtapot_h[Beta]\Release\Kol_8_h.pdb
E:\Projeler\Ahtapot\Source\Binder_h\Release\Binder_h.pdb
E:\Projeler\Ahtapot\Release\Ahtapot_h[Beta]\Release\Tohum_h.pdb
E:\Projeler\Ahtapot\Release\Ahtapot_h[Beta]\Release\Beyin_h.pdb
```

Campaign Infrastructure

```
blogg.serveblog[.]net
twiter.serveblog[.]net
messenger.serveirc[.]com
tigereyes2.servepics[.]com
driver.myftp[.]org
antivirus.myftp[.]org
adobupdate.serveftp[.]com
adobupdate.servehttp[.]com
```

Hashes

SHA256	Filename ITW	Component Type
784478fbb9a4755e303bad4f0b299a1f2c9704e71eb9579de65962827111b120	yok.scr	Bandook w/ Decoy Doc
a65f6da7df520e182d06b7b3a80485ce7a60dce503f349430d1e20ef9ca4ddb5	yok.rar	Infection Vector (Archive)
42b638b82891197e0028aef14862da00f52bdf044e17bb03d0f35289ba9774a9	AKP_oncesi-sonrasi.pdf	Infection Vector (Exploit PDF)
341e2dd4c65782a34fa0fa8225d957bef55d2e0330fc388359ace197a24067bf		Turkojan
210612fe4455bd663f314d7da8bb6bffe8d6a0e47092e288f71855afd1ecd7ae	RssReader2.1.zip	Infection Vector (Archive)
4c46e8f35ee5663cff59edcf6d5b9f51f491baf37079d33f8a24417c85a5cd9d	Duyuru.pdf	Infection Vector (Exploit PDF)
f748f51907267d3d30b39ff2fda937da19a06b25fe0a085a2203d1d43118a79e	AKPkarikaturleri.zip	Infection Vector (Archive)
81bb13258847cc141bd12b29971ef073126c42deb696b3ee18eda55c7ee2553f	1tayyip.scr	
Arsenal Samples not on VirusTotal (SHA1)		
61890ec3617cfdeaf736bf389fa0fe8e	belge.zip	
bf24a6e6ff11192391abe532452a5ba9	belge.scr	
Additional components not in Arsenal Report		
06e7dd7fac47ca5b7c732d780fcf1449f0f8d78fddf7ea7f16534812c8b99ad3	svchost.exe	Ahtapot Brain (Beyin)
664c9402f3a02710780980f2be5242eb9bf913f3527f15c798b48b89833b3ed2	windows.exe	Ahtapot Seed (Tohum)
8e6a75a009d9d27378b7e667080901503ad2913e12dfc0ec9491cda92d18c281	trp.exe	Ahtapot Arm (Kol)
09b06abb5f50978438f832f2fb2755c10838ff12810e3b1bdf487db9e0ceada0	BAYRAMINIZI KUTLARIZ.exe	Ahtapot Binder
c14d433b521ddf1981f2320a8276fb49ea2f03f0db3ca7de0de34a98b4955368	BAYRAMINIZI KUTLARIZ.rar	Infection Vector (Archive)
c52c2c6e02d4f2fce7f1e940e79bd3a4e12bae547df3efd226e8a8ae5279fb8f	bixitgpj.exe	Ahtapot Binder
9eddaa6ebe3f4e2dc51b245fc4603620272822c640d2dbe56960d8545d78e6f5	onemli.zip	Infection Vector (Archive)

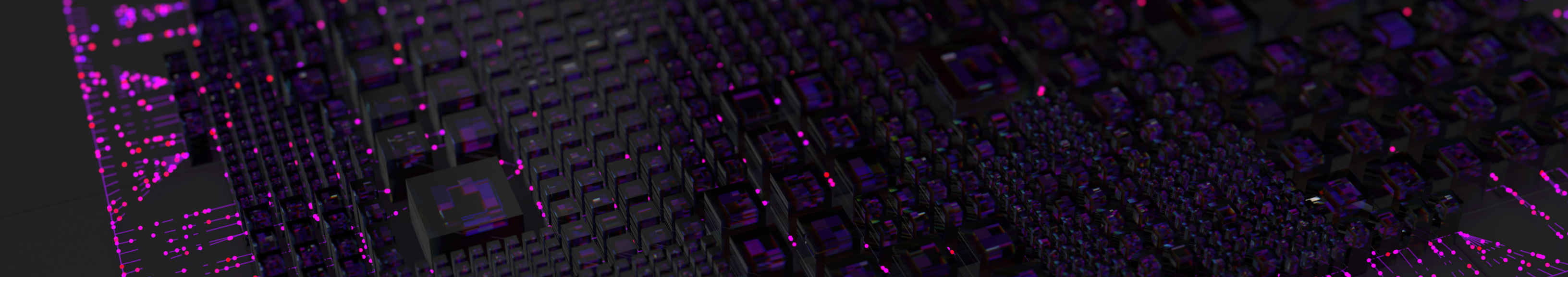
TECHNICAL APPENDIX B: RAD (2010-2015)

PDB Paths

```
J:\opt\project\vs2010\Rat\RatStarter\Release Md\RatStarter.pdb
C:\SEA\RadApplicationInstaller\Release\RadApplicationInstaller.pdb
J:\egm\egm_projes_int\vc\FileTrojen\Release\FileTrojen.pdb
J:\egm\egm_projes_int\vc2\RatStarter\Release Md\RatFileSystemModule.pdb
J:\egm\egm_projes_int\vc2\RatStarter\Release Md\RatScreenModule.pdb
J:\egm\egm_projes_int\vc2\RadApplicationInstaller\Release\RadApplicationInstaller.pdb
J:\egm\egm_projes_int\vc2\RatStarter\Release Md\RatStarter.pdb
J:\egm\egm_projes_int\vc2\RatStarter\Release Md\RatKeyboardModule.pdb
J:\egm\egm_projes_int\vc2\RatStarter\Release Md\RatBrowserModule.pdb
J:\egm\egm_projes_int\vc2\RatStarter\Release Md\RatSoundModule.pdb
J:\egm\egm_projes_int\vc2\RatStarter\Release Md\RatMailModule.pdb
```

Emails for Comms

```
tazekayisi@gmail.com
alisverisa@gmail.com
alisverisb@googlemail.com
lennjohn@yandex.com
johndown@woxmail.com
kanzaki@woxmail.com
michaelbrown2012@gmail.com
```



EGM hashes by Component Type

Infection Vectors

SHA256	Filename ITW
4cbb8e0bde66af241819c7492db0a9084b9c504dc3f69b7d8e5ef77198008991	*gercekler.rar*
5e02f7d0337750be8dd36c96638b8f44127d6fdabe5d7ae04b11fd3ca2d14de4	*Turkcell Müşteri Hizmetleri.eml*
dd60b8f2144de64ed1e2182d511d68ca0c60e1de0d8fa4a6bf80c9701c0ced52	*Turkcell_hediye.zip, Melih2.zip*

RadApplicationInstaller.pdb

SHA256	Filename ITW
92abdfa8d72cd42f6e6f3ad903380df5397e6ea8328c47422f8e016ee204f3bc	*start.exe*
b5b4a78ccc452052cddd85d1ba8c0d091d4836a2e1fa48785008515238a7a891	*resimler.scr* *(translates to 'pictures')*
f6c6d16c36b8f6942626abda7f8362db805c2fed9fccd069296825d7aeb9f4b7	*AdobeFlashPlayer.exe*
52123dbda7ca94e2a2938f220c7eeb825ada615c1c4c7ae3c364fe261c38d217	*gercekler.exe* *(translates to 'truths')*
33cd2aaab3ef17e4ec3d7fa9d73bafba7471a0e38cf56a9afba01b39dbbffa13	*AidforSYRIA.exe*
b79df7817ac1f39692927a593bf0569fd57e3faaebbbf4a0c7b452e7928157cb	*start.exe*
4e259d4e3527ef7eb359236d2eb36b5e42bec3e037684e0fdc4e077933b4b20f	*Süpperrr.scr*
3443090acf7b5a60070ba9b3ba07a8e340352779eec80ff28f454de660fb2787	*start3.exe.dat*
b3f183f941b5d30755bdc84e731cfc1f6c5e75650cb14dcf59ed90w183b3146c6	
3d3f208e54da010a571bc53296621428786cecb624f4c433d83dd4f40908820c	*turkcell_hediye.exe*
bcd5e2ac31b250e665691487f8eda0d2d170a4f31fad0aba158f73445351654f	
0a9357e9db888a601ade886fb54fa4eacdcfee72e3145dfbb26ae9492abfd877	

RatFileSystemModule.pdb

SHA256	Filename ITW
d5c7b3c8ec449057ec923672056153fc77d26eb240199cfa904c9cca6cf7142b	*WmiPrvSE.exe*
493bacf42bc9321f6b40b067fe3ef7fe83641f8d2c8dbca235ee22aa03da5d39	*WmiPrvSE.exe*
396c3f3dcbea740b230acd1b105db87fd282d313b68299cc3bb2e42c520effe0	
430b7a62da405562c4eb5a0aeada013b9c30d889ef0dc8fcc2efeebc90fb3045	*WmiPrvSE.exe*
b4d70c893a7871c204a7c2413a7b62fe9fe5fe3deecd28cf03b40a2b20c320a4	*WmiPrvSE.exe*
193ff40092196249fe8170b1a6dbd4974e7cb5080f9603d014b27b7f87102fac	*WmiPrvSE.exe*

RatKeyboardModule.pdb

SHA256	Filename ITW
182cbff13ef4149abdf0de2a78891fc403790913ce823a5f1ae59598f9609e9c	*SynTPHelper.exe*
421cab5cf169aafe8c9258a4e4089a345c8fa00164d158694ee799b00df054d4	*SynTPHelper.exe*
e855fa01f8f73a1bc9be78861f3ef1bb055ea2c627ab054161999f0dfe2faf09	*SynTPHelper.exe*
390824054cf068413036b0fdeb49aa5a17f0f0aac01bdbcd394db25f49b12edf	*SynTPHelper.exe*
0ad39d35ba9dcff65fe51329677acc9e8fe2f08e9e48e15361a132bd79d5acdc	*SynTPHelper.exe*
c2b042ecba51c2f3754eb43d79c5bbff7b27e9d5ddb96c9faa7bd067828a37fa	*SynTPHelper.exe*

RatStarter.pdb

SHA256	Filename ITW
588f3edabde316ad7e885884873c93863499bd741f7dcd5009e74a84b6debc6e	*wsms.exe*
a82a80f53a65f8a3c0b39b82d178897e9f5ef3a22286b567a38c242d17098a68	*wsms.exe*
bac99daa5276cc152c326a1d1fd5ecadd45e4cb412665156e3c7c70ebde9fd62	
0ebcb9184d191bbd442d6318b39ea756778bb0a89a52c63e1ddff7497011f480	*wsms.exe*
9ae44842c8db8cfb084d86cf9b0fec62c9c0d559326f86d7008edb90d5596221	*wsms.exe*
e35c24d485c43aad17d42ded594fc1d54d7a5058fea2ab3cd481e927bbfcc58f	*wsms.exe*

RatBrowserModule.pdb

SHA256	Filename ITW
c65e2f59de1bc202cc18d91e12b3abb797027a3b99a61db9dfa9789ded8501c6	*TService.exe*
6fdf2463d4f3bbfe37862c0b58d3104a46d6f31333fd7370e1e4e4c28d114092	*TService.exe*
a0c384e633106cbdf88ed7d808bb947ece1e0ffa11568c21c751da3d650e4f50	
bb3851f70ffbb82d263a4d442a288552a23f0c3bdd2f7b6bfbd4cd626a04efd1	*TService.exe*
ff94e44a87f7603df2227c77485b81044627d55289c7b553463e2064aac74854	*TService.exe*

RatSoundModule.pdb

SHA256	Filename ITW
3bddc611b3e55d0e3356f22daff5e4002a9bde0709210d9e758e2e0cc22921b9	*VolCtrl.exe*
b17038613b421643adf9378fa9359894e21c6655c2561581bc844e3a01228be6	
8ffa3971ca730973c02aa6fe47c50bd79ef30664ec996dfe14e757711f8da070	*VolCtrl.exe*
64c335f2344d23aaff34c9ab4d7b9229c7bc4d76ae86e451baa29f65f9266266	*VolCtrl.exe*
4ae3d5c447ba7ec536b9f7a6f2d274e1921d3832f276a71244f811141e1dcc4b	*VolCtrl.exe*

RatMailModule.pdb

SHA256	Filename ITW
ecf4685f6110381a8f37bb0e8857b324d0c12bfcc9b95b6b00e54a4b3d71d182	*SearchIndexer.ex*
7e0e8e0ab797648aad8fdbab4687249c6f8c00262083c63f44779ef43d0b38ed	
b4108cf9ecd6b2594cf2b39f53df5531f7a3aea2762f2439e0bc666935067c44	*SearchIndexer.ex*
13444cfcd1fd8bb66e20cd16d8f740355813401e2a682b3a84ab5975fab6580e	*SearchIndexer.ex*
96922c8b94f6a539e21ba4df8959b75eadd1eae994d25dc4f95db30e161d8937	*SearchIndexer.ex*
1837d3d8aa0c3773a4711bb5f9a8765701b9467c916b3a61df18472ffed57944	*SearchIndexer.ex*

FileTrojen.pdb

SHA256	Filename ITW
1a06fe56c6788778de958c04c9fca90c8bcbb5eace63ae759cdde541eca82560	*gercekler.rar*
785be60227fd1a597497051ffe3a5d13b15dfd979169154c6c9228c9c6d0cda9	*Embedded Powerpoint Lure*

RatScreenModule.pdb

SHA256	Filename ITW
1bdaebfd3f05156fcf968cad312bed0f69f953125a0912a5b2663f9407844885	*QLBCtrl.exe*
9bbbbaa2be803bcc8f2fdbff0f2c137b02ab089bb7c36d1df7da821ed9294f31	
e3a712d65a187c1a4a8381cb0347504705099665c7c9abe29e0be72c704dd80a	*QLBCtrl.exe*
8d5618388cdd859deffc51a9d07a87af3871d916a6d9544796346abdd9a2250d	*QLBCtrl.exe*
32a3ef2ded4cb1bd2d1a18146d71eb3152df4bec0bb2ffb4f58b25f47c73d307	*QLBCtrl.exe*

SHA256	Filename ITW
51078001db7aa722ad796527bc289c2f697c54df388319b98a42b48e717573c8	*Microsoft.CAB_*
f8be54eab9ac3484eb5e626e43691b380d25b293df84aa995d6febb28fa4a8b1	*Microsoft.CAB.dat*

TECHNICAL APPENDIX C: HACKING TEAM (2013)

Watermarks

RCS Version	TNP Watermark
Pre 9.2	*ZjvOuN3m*
Post 9.2	*IdQcUI52*

Hashes

SHA256
04d659739849d16c2e75c803b67f88cb54a722335625b7b509407a52f7e6003e
0a786bfcee6e1ad12bd9cae585e5bbbd7a05c02b4aadb0fc660880f931c23e6a
139958f77cf97d879185613a546c489a1026aacceb966f5242d80dc6e0f29ec7
26271b82e892a8fdcd3e9e3141f3893dd8f60bc2a2c4a958f77cb3159b64471d
4d632459ed7f2a4f6f89f72cfe6bf834052dbeddca72e7a96798132895b62a66
8303321cd9389ec20ae0df8dc5f8d69d598b63e27e3a80ec3ec2fbfe4ec3a796
b18793cb17b9bb8fdb89c60491584bf79fac95f85783ab1a53cb5b351918f2e2
b1bb0108cad31bdc127fa4bcb133f5f0311c7c8ff950a822502596350eeed944
b30e2d39ad6dc94d9c2995c5db38ab406d4475ff22a68a26ebaeeb5240fb17de
b45bd4f6a7a5ba26b194dc6ac5ec2b5b6e0160c2944b99c1acd06a92be941364
e0be88ec83d63823f5fde48002131a6f2fa5e4a232a55ecf1d5630dbbfa2bd9d
ecb4779c87ea2c0a95ccd1d0231ba063e4b53d86d28b29d0566a8ef0192f485d

Campaign Infrastructure

46.251.239.67	*Anonymizer VPS*
199.175.51.16	*Anonymizer VPS*
146.185.30.109	*Anonymizer VPS*
46.166.167.215	*Anonymizer VPS*
http://halkinsesitv[.]com	*Collector*
212.57.8.226	*Collector*
95.9.71.180	*Collector*
46.183.220.222	*Collector*

Yara Rules

```
rule apt_TR_EGOMANIAC_quirks
{
      meta:
              desc = "Quirks in RatMailModule"
              author = "JAG-S @ SentinelLabs"
              version = "1.0"
              TLP = "White"
              last_modified = "04.09.2021"

      strings:
              $misspelled1 = "There is end for not written area." ascii wide
              $misspelled2 = "dirvefixed" ascii wide
              $misspelled3 = "Resource can not be readed" ascii wide

              $mutex = "Project1_MutexNameForTerminator" ascii wide

              $turkish_usage1 = "Tus kaydi basladi. Dosya:" ascii wide
              $turkish_usage2 = "Cikmak icin ENTER tusuna basiniz." ascii wide
      condition:
              uint16(0) == 0x5a4d
              and
              any of them
}

rule apt_TR_EGOMANIAC_driveList
{
      meta:
              desc = "Drive params"
              author = "JAG-S @ SentinelLabs"
              version = "1.0"
              TLP = "White"
              last_modified = "04.09.2021"

      strings:
              $ = "drivewindows" ascii wide
              $ = "currentuserdesktop" ascii wide
              $ = "currentuserdocuments" ascii wide
              $ = "currentuser" ascii wide
              $ = "windows" ascii wide
              $ = "programfiles" ascii wide
              $ = "currentappdata" ascii wide
              $ = "currentexplorercookies" ascii wide
              $ = "currentexplorerhistory" ascii wide
              $ = "allprofiles" ascii wide
              $ = "driveremovable" ascii wide
              $ = "mycomputer" ascii wide
              $ = "dirvefixed" ascii wide
              $ = "drivefloppy" ascii wide
              $ = "driveremote" ascii wide
              $ = "drivecdrom" ascii wide

      condition::
              uint16(0) == 0x5a4d
              and
              all of them
}

rule apt_TR_EGOMANIAC_configFilenames
{
      meta:
              desc = "Config specifics"
              author = "JAG-S @ SentinelLabs"
              version = "1.0"
              TLP = "White"
              last_modified = "04.09.2021"

      strings:
              $filename1 = "work.exe is not located in normal path" ascii wide
              $filename2 = "start.exe" ascii wide
              $filename3 = "output" ascii wide
              $filename4 = "conf.properties" ascii wide
              $filename5 = "Microsoft.conf" ascii wide

      condition:
              uint16(0) == 0x5a4d
              and
              all of them
}

rule apt_TR_EGOMANIAC_RadFuncs
{
      meta:
              desc = "Rad Function Names"
              author = "JAG-S @ SentinelLabs"
              version = "1.0"
              TLP = "White"
              last_modified = "04.09.2021"

      strings:
              $rad1 = "RadUnknownParameterException" ascii wide
              $rad2 = "RadWrongParameterException" ascii wide
              $rad3 = "RadParseException" ascii wide
              $rad4 = "RadFileNotFoundException" ascii wide
              $rad5 = "RadDbConnectionException" ascii wide
              $rad6 = "RadFetalException" ascii wide
              $rad7 = "RadResourceException" ascii wide
              $rad8 = "RadNotImplementedException" ascii wide
              $rad9 = "RadSystemCallException" ascii wide
              $rad10 = "RadWindowsLastErrorException" ascii wide
              $rad11 = "RadStdioException" ascii wide
              $rad12 = "RadFileIsBusyException" ascii wide
              $rad13 = "RadSqliteLockedException" ascii wide
              $rad14 = "RadNotEnabledModuleException" ascii wide
              $rad15 = "RadInterruptedException" ascii wide
              $rad16 = "RadSingletonException" ascii wide
              $rad17 = "RadDailyLimitReachedException" ascii wide
              $rad18 = "RadNullPointerException" ascii wide
              $rad19 = "RadMutexCanNotBeLockedException" ascii wide

      condition:
              uint16(0) == 0x5a4d
              and
              any of them
}

rule apt_TR_EGOMANIAC_pdbs
{
      meta:
              desc = "PDB path generics"
              author = "JAG-S @ SentinelLabs"
              version = "1.0"
              TLP = "White"
```

```
                last_modified = "04.09.2021"

        strings:
                $pdb_gen = "J:\\egm\\egm_projes_int\\vc" ascii wide
                $pdb_gen2 = "\\RatStarter\\Release Md\\" ascii wide
                $pdb_gen3 = "C:\\SEA\\RadApplicationInstaller\\" ascii wide

        condition:
                uint16(0) == 0x5a4d
                and
                any of them
}

rule apt_TR_EGOMANIAC_components
{
        meta:
                desc = "Component internal references"
                author = "JAG-S @ SentinelLabs"
                version = "1.0"
                TLP = "White"
                last_modified = "04.09.2021"

        strings:
                $component1 = "file-search" ascii wide
                $component2 = "browser" ascii wide
                $component3 = "key-logger" ascii wide
                $component4 = "screen-capturer" ascii wide
                $component5 = "sound-record" ascii wide
                $component6 = "sender" ascii wide
                $component7 = "working-type" ascii wide
                $component8 = "mydeleter.bat" ascii wide
                $component9 = "RatApplication" ascii wide
                $component10 = "DCApplication" ascii wide

        condition:
                uint16(0) == 0x5a4d
                and
                8 of them
}

rule apt_TR_EGoManiac_HT
{
        meta:
                desc = "HackingTeam samples related to TNP Ops"
                author = "JAG-S @ SentinelLabs"
                last_modified = "09.02.2021"
                version = "2.0"
                TLP = "White"
                reference = "https://wikileaks.org/hackingteam/emails/emailid/506779"
        strings:
                $watermark1 = "ZjvOuN3m" ascii wide //pre 9.2
                $watermark2 = "IdQcUI52" ascii wide //post 9.2
```

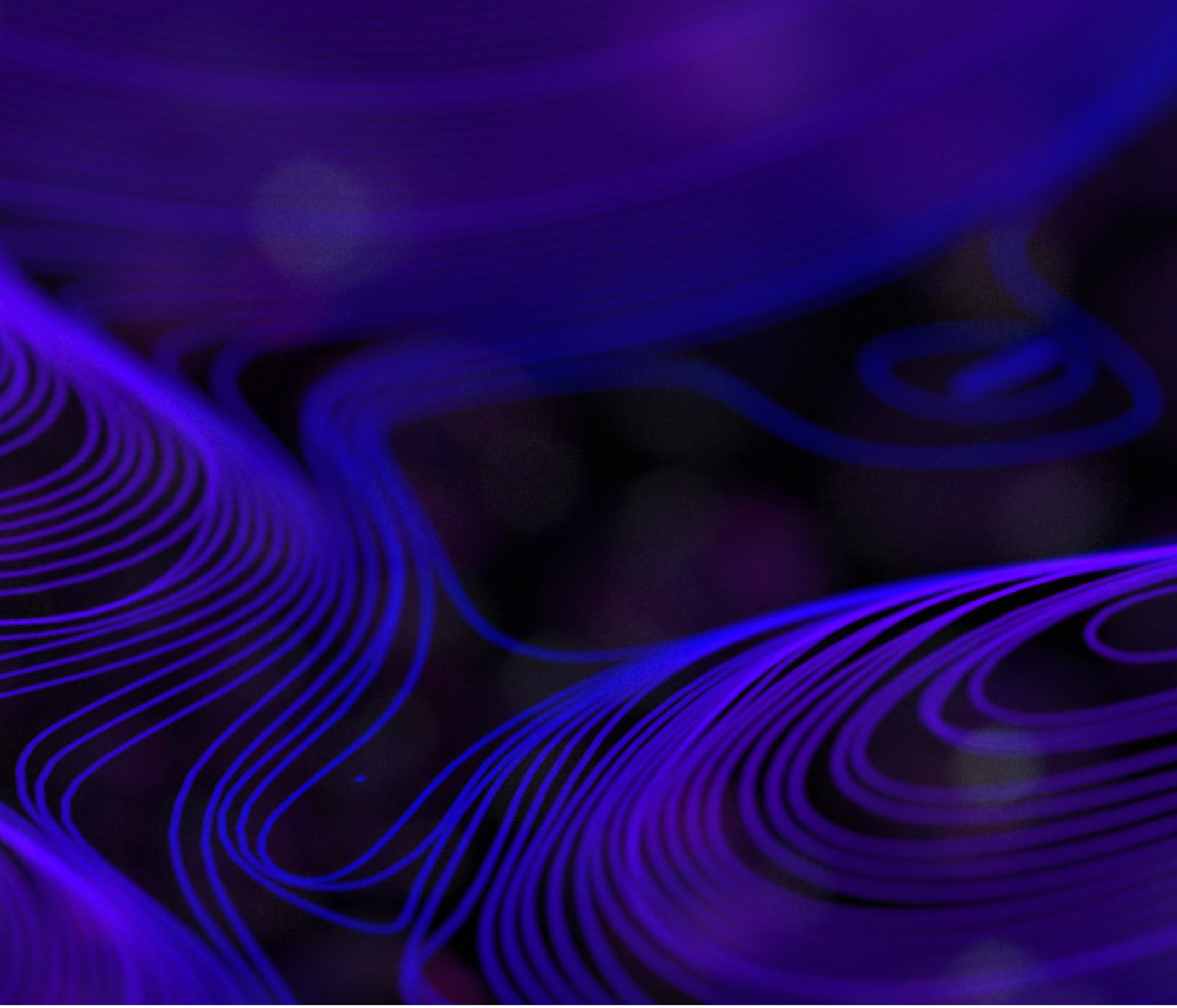
```
$ip1 = "146.185.30.109" ascii wide
              $ip2 = "46.183.220.222" ascii wide
              $ip3 = "46.251.239.67" ascii wide
              $ip4 = "199.175.51.16" ascii wide
              $ip5 = "46.166.167.215" ascii wide

              $path = "/dispatch.asp" ascii wide

              $htTell1 = "Engine started" ascii wide fullword
              $htTell2 = "Running in background" ascii wide fullword
              $htTell3 = "Stale thread" ascii wide fullword
              $htTell4 = "The current thread is probably stale!" ascii wide fullword
              $htTell5 = "Locking doors" ascii wide fullword
              $htTell6 = "Rotors engaged" ascii wide fullword
              $htTell7 = "I'm going to start it" ascii wide fullword
              $htTell8 = "I'm going to start the program" ascii wide
              $htTell9 = "I'm going to start the program automatically, is it ok?" ascii wide
              $htTell10 = "Starting upgrade!" ascii wide

              $drops1 = "%s\\%S*tmp" ascii wide fullword
              $drops2 = "%s\\%s%x%x.tmp" ascii wide fullword
              $drops3 = "%s\\%d.bat" ascii wide fullword
              $drops4 = "%s\\%S.exe" ascii wide fullword
              $drops5 = "%s\\%s.tmp" ascii wide fullword

              $gather1 = "CPU: %d x %s" ascii wide fullword
              $gather2 = "RAM: %dMB free / %dMB total (%u%% used)" ascii wide fullword
              $gather3 = "Hard Disk: %dMB free / %dMB total" ascii wide fullword
              $gather4 = "Windows Version: %s%s%s%s%s" ascii wide fullword
              $gather5 = "Registered to: %s%s%s%s {%s}" ascii wide fullword
              $gather6 = "Locale: %s_%s (UTC %.2d:%.2d)" ascii wide fullword
              $gather7 = "User Info: %s%s%s%s%s" ascii wide fullword
              $gather8 = "Application List (x86):" ascii wide fullword
              $gather9 = "ApplicationList (x64):" ascii wide fullword
              $gather10 = "SID: %s" ascii wide fullword
      condition:
              uint16(0) == 0x5a4d
              and
        any of ($watermark*)
        and
        (
              any of ($ip*)
              or
              $path
              or
              any of ($htTell*)
              or
              all of ($drops*)
              or
              5 of ($gather*)
        )
}
```



ABOUT SENTINELLABS

InfoSec works on a rapid iterative cycle where new discoveries occur daily and authoritative sources are easily drowned in the noise of partial information. SentinelLabs is an open venue for our threat researchers and vetted contributors to reliably share their latest findings with a wider community of defenders. No sales pitches, no nonsense. We are hunters, reversers, exploit developers, and tinkerers shedding light on the world of malware, exploits, APTs, and cybercrime across all platforms. SentinelLabs embodies our commitment to sharing openly –providing tools, context, and insights to strengthen our collective mission of a safer digital life for all. In addition to Microsoft operating systems, we also provide coverage and guidance on the evolving landscape that lives on Apple and macOS devices. https://labs.sentinelone.com/