



MERTSARICA

CYBER SECURITY RESEARCHER

UYARI.

Bu sunum, FireEye reklamı yapmak amacıyla hazırlanmamıştır!

Bu sunumda anlatılanların hiçbiri hayal ürünü değildir!

Siz bu sunumu izlerken birileri kurumunuzu hedef alıyor olabilir!



İÇERİK.

APT Nedir ?

APT ile Nasıl Mücadele Edilir ?

Bir APT Girişimi

Sonuç



BEN KİMİM?

Uzmanlık Alanlarım _____ Sızma Testi, Zararlı Yazılım Analizi, Bilgisayar Olaylarına Müdahale

Blog Yazarı _____ www.mertsarica.com

Güvenlik TV _____ www.guvenliktv.org

Sertifika Koleksiyoncusu _____ CISSP , SSCP , OSCP , OPST , CREA, CERE



MESLEĞİM.

QNB Finansbank'ın Bilgi Teknolojileri iştiraki olan IBTech firmasında, Tehdit ve Zafiyet Yönetimi ekibinde Teknik Lider olarak görev yapmaktayım. (2007 - *)

www.ibtech.com.tr

www.qnbfinansbank.com



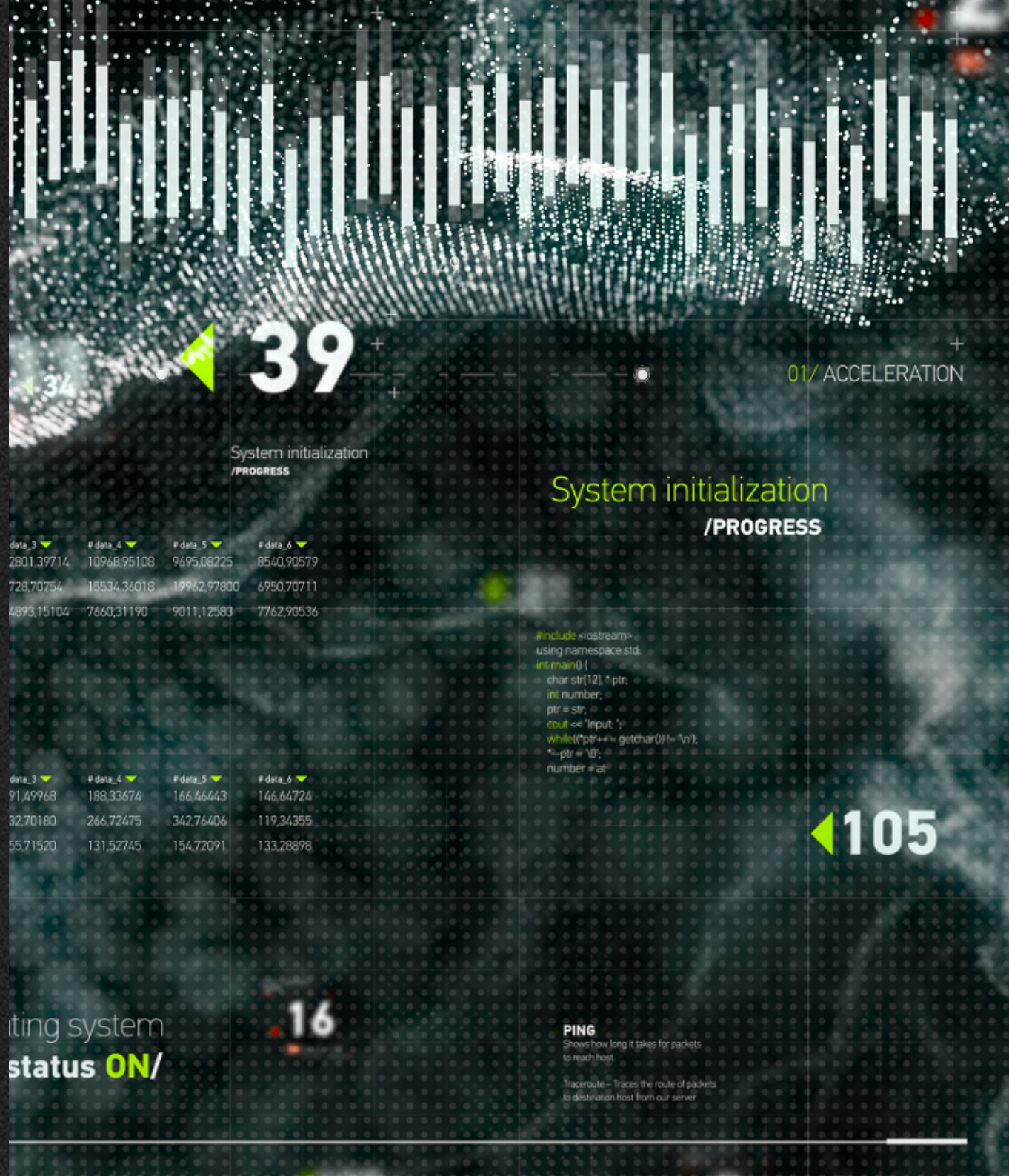
APT NEDİR ?

Kurumunuzu ve çalışanlarınızı hedef alan organize siber saldırıdır.

İleri seviye saldırı yöntemleri & zararlı yazılımla kullanılmaktadır.

Geleneksel güvenlik çözümleri yetersiz kalmaktadır.

Farketmesi zor, müdahale ve analiz etmesi daha da zordur.



“Taktik, yapacak bir şey varken ne yapılması gerektiğini bilmek;
Strateji ise yapacak hiçbir şey yokken ne yapmak gerektiğini bilmektir.”

Savielly Tartakower

APT İLE MÜCADELE KANUNU.

Çalışanlara ve uzmanlaşmaya yatırım

Teknolojiye yatırım

Vizyon & üst yönetim desteği



“Her zaman en tembel insanları işe alırım çünkü tembeller çok karışık işleri bile en kısa yoldan yaparlar.”

Bill Gates

ÇALIŞANLARA YATIRIM.

Cihazları ve sistemleri insanlar yönetir.

Çalışan ne kadar eğitilmiş olur ise siber saldırı tespitinde ve müdahalesinde o kadar başarılı olur.

Ne iş olursa yapana değil, işini iyi yapana yatırım yapılmalıdır!



TEKNOLOJİYE YATIRIM.

Doğru zamanda doğru teknolojiye yatırım yapılmalıdır. (Sandbox, IDR vb.)

Tehdit raporları (Mandiant vb.), önceliklendirmeniz gereken yatırımlar konusunda size ışık tutacaktır.

Ürün seçiminde alarm sayısı değil, doğru alarm sayısı önemlidir!



VİZYON & ÜST YÖNETİM DESTEĞİ.

Çalışanlarınıza kulak verin.

Yatırımlarınızı ötelemeyin.

Başkalarının hatalarından ders çıkarın. (XBank, YBank, vb.)

Harekete geçmek için **hacklenmeyi** beklemeyin!



NEDEN KUM HAVUZU SİSTEMİ?

Kurumunuzda çok sayıda güvenlik sistemi/ cihazı var.

Çok sayıda da güvenlik alarmı var! (f/p, korelasyon eksikliği)

Statik ve dinamik olarak dosyaları analiz eden bir teknoloji sayesinde az, öz, önemli alarmlara odaklanabilirsiniz.



FİREEYE TECRÜBELERİM.

2014 yılından bu yana **FireEye'in NX** ürününü kullanıyorum.

Bu zamana dek **False Positive** diye itiraz ettiğim 3 vakada da yanılan ben oldum. :)

Son 10 yılda tanık olduğum en ciddi siber saldırı girişimlerini (APT), **FireEye NX** tespit etti.



APT GİRİŞİMİ 1.



TARİHÇE.

08.12.2016 – Hacker, w.frost@lse.ac.uk adresinden üst düzey bir yetkiliye e-posta gönderiyor.

09.12.2016 – Yazışmaların sonunda hacker, zararlı kod içeren ofis dokümanının bulunduğu adresi üst düzey yetkiliye gönderiyor.

09.12.2016 – FireEye NX, vekil sunucu (proxy) trafiği üzerinden zararlı kod içeren ofis dokümanını tespit ediyor ve engelliyor!

09.12.2016 – Zararlı yazılım analizi süreci başlatılıyor.



APT GİRİŞİMİ #1

My name is [REDACTED], I work at the London School of Economics.

I am the head of the jury panel of contests organized by The Banker: <http://www.thebanker.com/>
Jury panel consists of representatives of several leading universities and also high-qualification experts from the financial corporations.
Recently, one place in the expert group has become vacant.

We are looking for a consultant that could help us to assess candidates for Islamic Bank of the Year Awards: <http://www.thebanker.com/Awards/Islamic-Bank-of-the-Year-Awards>
They must have the experience in banking service and sufficient knowledge at the specifics of the region.

It's great honor for me to invite you to join our team.

Are you interested in participation?

Best,

1

APT GİRİŞİMİ #1

2

The Banker Awards contest is held not the first time. Best scientists of the University College London, University of Miami School of Business Administration and other universities are the main experts. Jury panel is regularly updated. External advisor group consists of 20 people – there is one vacant place now.

You will have to answer the set of questions regarding nominees of Islamic Bank of the Year Awards. It is essential for more precise assessment of candidates in each nomination.

At the average, it may take about 2-3 hours a week. We provide flexible work hours and remote work opportunities.

In return, you will get the certificate of the honored contest expert, and prospect for further development in this direction.

In next 3 weeks, we will need your assistance. If it goes well, we will proceed cooperation in 2017.

What do you think?

Best,

APT GİRİŞİMİ #1

Foremost, you have to fill out and send me the Expert application form:

http://moya.bus.miami.edu/~emil/Documents/Application_Form.doc

Further, I will prepare the NDA. After that, I will send you first questions.

Best,



APT GİRİŞİMİ #1

Acknowledge the infections and callbacks above for the host at [redacted]

[redacted] [redacted] 5 4 1 0 Malware.archive 12/09/16 16:19:00

Malicious Capabilities Observed in the VM

Malicious Behavior: Yes

- Generic Trojan Behavior
- Suspicious Persistence Activity
- Suspicious Persistence Behavior

OS Change Summary

Malware detected

| Malware | Severity | Total | Infections | Callbacks | Blocked | Botnets | Last CnC Server | Last Location | First Seen | Last Seen | Ports Used | Protocols |
|--|----------|-------|------------|-----------|---------|---------|-----------------|---------------|-------------------|-------------------|------------|-----------|
| Malware.archive | ■■■■■ | 2 | 2 | 0 | 0 | 0 | | | 12/09/16 15:30:30 | 12/09/16 16:19:00 | 8080 | TCP |
| Local.Callback | ■■■■■■■ | 1 | 0 | 1 | 0 | 1 | | | 12/09/16 15:30:47 | 12/09/16 15:30:47 | 8080 | TCP |
| Heuristic.APT.Possible_PoisonIvy_Handshake | ■■■■■■■ | 1 | 1 | 0 | 0 | 0 | | | 12/09/16 15:30:30 | 12/09/16 15:30:30 | 8080 | TCP |

Malware Binaries

| Md5sum | Filetype | Protocol | Encoding | Last analysis time | # Occurrences |
|----------------------------------|----------|------------|----------|--------------------|---------------|
| b7409525256529be43a51851e0bb6617 | zip | TCP (8080) | | 12/09/16 15:30:30 | 1 |
| 1be9799d85fedfcbab8a95c5e50262e | dual | TCP (8080) | | 12/09/16 16:19:00 | 2 |
| 796dff8007f3163adfc9fa7f5fde1c | exe | TCP (8080) | | 12/09/16 15:30:30 | 1 |

Acknowledge the infections and callbacks above for the host at [redacted]

[redacted] [redacted] 2 2 0 0 Malware.archive 12/09/16 14:53:56

Malware detected

| Malware | Severity | Total | Infections | Callbacks | Blocked | Botnets | Last CnC Server | Last Location | First Seen | Last Seen | Ports Used | Protocols |
|-----------------|----------|-------|------------|-----------|---------|---------|-----------------|---------------|-------------------|-------------------|------------|-----------|
| Malware.archive | ■■■■■ | 2 | 2 | 0 | 0 | 0 | | | 12/09/16 14:53:56 | 12/09/16 14:53:56 | 8080 | TCP |

Malware Binaries

| Md5sum | Filetype | Protocol | Encoding | Last analysis time | # Occurrences |
|---------------------------------|----------|------------|----------|--------------------|---------------|
| 1be9799d85fedfcbab8a95c5e50262e | dual | TCP (8080) | | 12/09/16 14:53:56 | 2 |

APT GİRİŞİMİ #1

Application_Form.doc - Word

FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW VIEW Sign in

Clipboard Font Paragraph Styles Editing

SECURITY WARNING Some active content has been disabled. Click for more details. Enable Content

Form number: 000034/16

Expert Application Form

This form is processed automatically. Please use appropriate fields for your answers.

Name

Phone

E-mail

Q1. How long have you been working in the Banking field?

Less than a year 1 year - 3 years 3 years - 7 years More than 7 years

Q2. What is your specialty?

Q3. How would you rate you team working skills?

Very good Good Satisfactory Fair

Q4. How much time can you spend on the Cooperation tasks per week?

2-3 hours 4-6 hours 7-9 hours More than 9 hours

Q5. Do you have any professional certificates?

Yes No

Application_Form.doc 1.503 characters (an approximate value). %100

APT GİRİŞİMİ #1

Antivirus scan for f2c1 x

← → ↻ 🔍 <https://www.virustotal.com/en/file/f2c14c38122a6e0f5833fee794399f0341d9b96de954f762e32c0c9f8197535d/analysis/> ☆ ☰

Apps For quick access, place your bookmarks here on the bookmarks bar. [Import bookmarks now...](#)

Community Statistics Documentation FAQ About English Join our community Sign in

virustotal

SHA256: f2c14c38122a6e0f5833fee794399f0341d9b96de954f762e32c0c9f8197535d

Detection ratio: 0 / 53

Analysis date: 2016-12-09 11:59:53 UTC (21 hours, 4 minutes ago)

📊 0 📈 0

Analysis Additional information Comments 0 Votes

| Antivirus | Result | Update |
|------------------|--------|----------|
| ALYac | ✓ | 20161209 |
| AVG | ✓ | 20161209 |
| AVware | ✓ | 20161209 |
| Ad-Aware | ✓ | 20161209 |
| AegisLab | ✓ | 20161209 |
| AhnLab-V3 | ✓ | 20161209 |
| Alibaba | ✗ | 20161209 |
| Antiy-AVL | ✓ | 20161209 |
| Arcabit | ✓ | 20161209 |
| Avast | ✓ | 20161209 |
| Avira (no cloud) | ✓ | 20161209 |

APT GİRİŞİMİ #1

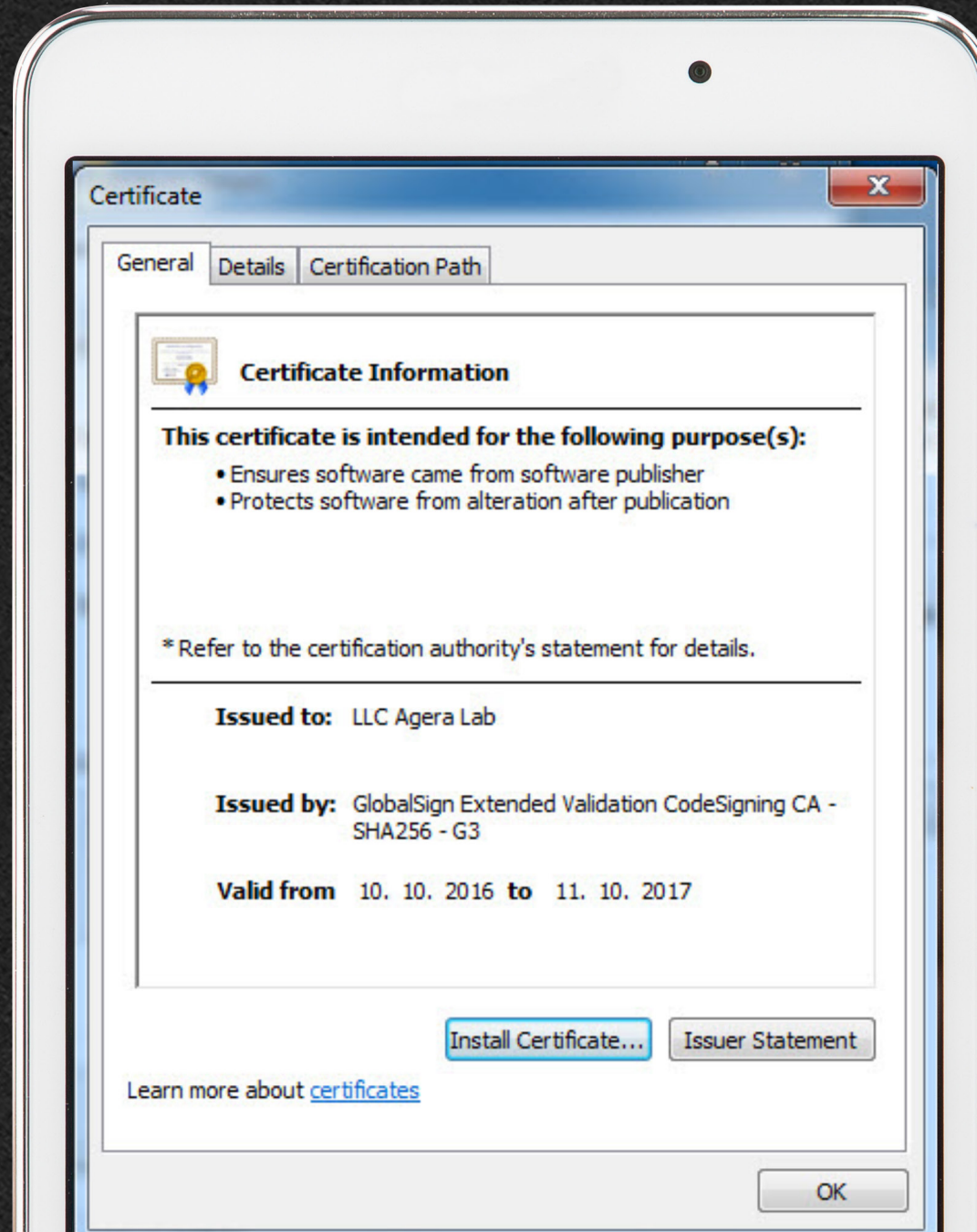
The screenshot shows the IDA Pro interface for the file 'nac132.idb'. The 'Functions window' on the left lists several subroutines, with 'start' selected. The 'Strings window' on the right displays a table of strings found in the binary. The 'Output window' at the bottom shows a message from the 'ApplyCalleeType' plugin.

| Address | Length | Type | String |
|-----------------|----------|---------|--------------------------|
| .rdata:00D9B4B0 | 00000008 | unic... | Run |
| .rdata:00D9B4D0 | 0000001E | unic... | CurrentVersion |
| .rdata:00D9B510 | 00000010 | unic... | Windows |
| .rdata:00D9B530 | 00000014 | unic... | Microsoft |
| .rdata:00D9B570 | 00000012 | unic... | Software |
| .rdata:00D9B5D0 | 00000010 | unic... | dd*.ddt |
| .rdata:00D9B5F0 | 00000010 | unic... | kk*.kkt |
| .rdata:00D9B610 | 00000010 | unic... | aa*.aat |
| .rdata:00D9B630 | 00000010 | unic... | ss*.sst |
| .rdata:00D9B6B0 | 00000024 | unic... | ddMMyy-HHmms-zzz |
| .rdata:00D9B6F0 | 0000000E | unic... | ddMMyy |
| .rdata:00D9B850 | 00000032 | unic... | application/octet-stream |
| .rdata:00D9B8B0 | 0000001A | unic... | Content-Type |
| .rdata:00D9B930 | 00000018 | unic... | aa%1-%2.aat |
| .rdata:00D9B970 | 00000014 | unic... | audio/pcm |
| .rdata:00D9B9F0 | 0000000A | unic... | JPEG |
| .rdata:00D9BDF0 | 00000012 | unic... | kk%1.kkt |
| .rdata:00D9BE14 | 00000006 | unic... |]\n |
| .rdata:00D9BE2C | 00000008 | unic... | \n\n[|
| .rdata:00D9BE44 | 0000000A | unic... | 0x%1 |
| .rdata:00D9BE60 | 00000008 | unic... | f%1 |
| .rdata:00D9BE78 | 0000000A | unic... | zoom |

```
gcc: not found
```

```
ApplyCalleeType: Starting up
ApplyCalleeType: Using ea: 0x009c8f11
ApplyCalleeType: Cannot (or shouldn't) run when call optype is o_near
Pattern "gcc" was not found.
```

APT GİRİŞİMİ #1



APT GİRİŞİMİ #1

From Linux to Windows – New Family of Cross-Platform Desktop Backdoors Discovered

By [Stefan Ortloff](#) on January 29, 2016. 3:52 pm

RESEARCH

BACKDOOR LINUX MALWARE DESCRIPTIONS NON-WINDOWS MALWARE SIGNED MALWARE

Background

Recently we came across a new family of cross-platform backdoors for desktop environments. First we got the Linux variant, and with information extracted from its binary, we were able to find the variant for Windows desktops, too. Not only that, but the Windows version was additionally equipped with a valid code signing signature. Let's have a look at both of them.

DropboxCache aka Backdoor.Linux.Mokes.a

This backdoor for Linux-based operating systems comes packed via UPX and is full of features to monitor the victim's activities, including code to capture audio and take screenshots.

```
$ file DropboxCache
DropboxCache: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, stripped
```

After its first execution, the binary checks its own file path and, if necessary, copies itself to one of the following locations:

- \$HOME/\$QT-GenericDataLocation/.mozilla/firefox/profiled
- \$HOME/\$QT-GenericDataLocation/.dropbox/DropboxCache

One example would be this location: \$HOME/.local/share/.dropbox/DropboxCache. To achieve persistence, it uses this not very stealthy method: it just creates a .desktop-file in \$HOME/.config/autostart/\$filename.desktop. Here's the template for this:

COULD YOUR BUSINESS SURVIVE A CRYPTOR?

Learn how to guard against crypto-ransomware

APT GİRİŞİMİ 2.



TARİHÇE.

28.02.2017 – Hacker, m.salvalaggio@lse.ac.uk adresinden aynı üst düzey yetkiliye ekinde dosya olan bir e-posta gönderiyor.

28.02.2017 – lse.ac.uk adresi ilk APT girişimi sonrasında kurum genelinde yasaklandığı için üst düzey yetkiliye e-posta ulaşmıyor.

28.02.2017 – SOC ekibi lse.ac.uk uzantılı e-posta adreslerinden gönderilen e-postaları yakından takip ettiği için alarm oluşuyor.

28.02.2017 – Zararlı yazılım analizi süreci başlatılıyor.



APT GİRİŞİMİ #2

Hello,

Congratulations, your candidature is approved.

The attachment contains the copy of the confirmation letter. Please pay attention to the expiry period of the certificate. You will get the hard copy via mail within 2 weeks.

Let's schedule a call on Thursday, 2 PM, do you mind?

Best regards,
Matteo

Matteo Salvalaggio
Senior Director of Development
London School of Economics & Political Science
Tel: +442039051983
Email: m.salvalaggio@lse.ac.uk

APT GIRISIMI #2

The image shows a screenshot of a LinkedIn profile for Matteo Salvalaggio. The browser address bar indicates the URL is <https://www.linkedin.com/in/matteo-salvalaggio-96635711a/>. The profile header features a blue background with a network diagram. The profile picture is a circular portrait of a man with a beard. Below the picture, the name "Matteo Salvalaggio" is displayed, followed by the current position: "Assegnista borsa di ricerca ReLuis presso Università degli Studi di Padova". A red arrow points to this text. Below the name and position, the text "Università degli Studi di Padova • Università degli Studi di Padova" and "Rovigo Area, Italy • 129" is visible. Two buttons, "Send InMail" and "Connect", are located below the profile information. The "Experience" section is visible below, listing two roles: "Assegnista borsa di ricerca ReLuis" at the University of Padua (Feb 2017 - Present) and "Assegnista borsa di ricerca PON-METRICS" at the University of Padua (Jun 2016 - Dec 2016).

Matteo Salvalaggio

Assegnista borsa di ricerca ReLuis presso Università degli Studi di Padova

Università degli Studi di Padova • Università degli Studi di Padova

Rovigo Area, Italy • 129

Send InMail Connect

Experience

Assegnista borsa di ricerca ReLuis
Università degli Studi di Padova
Feb 2017 - Present • 2 mos • Padova

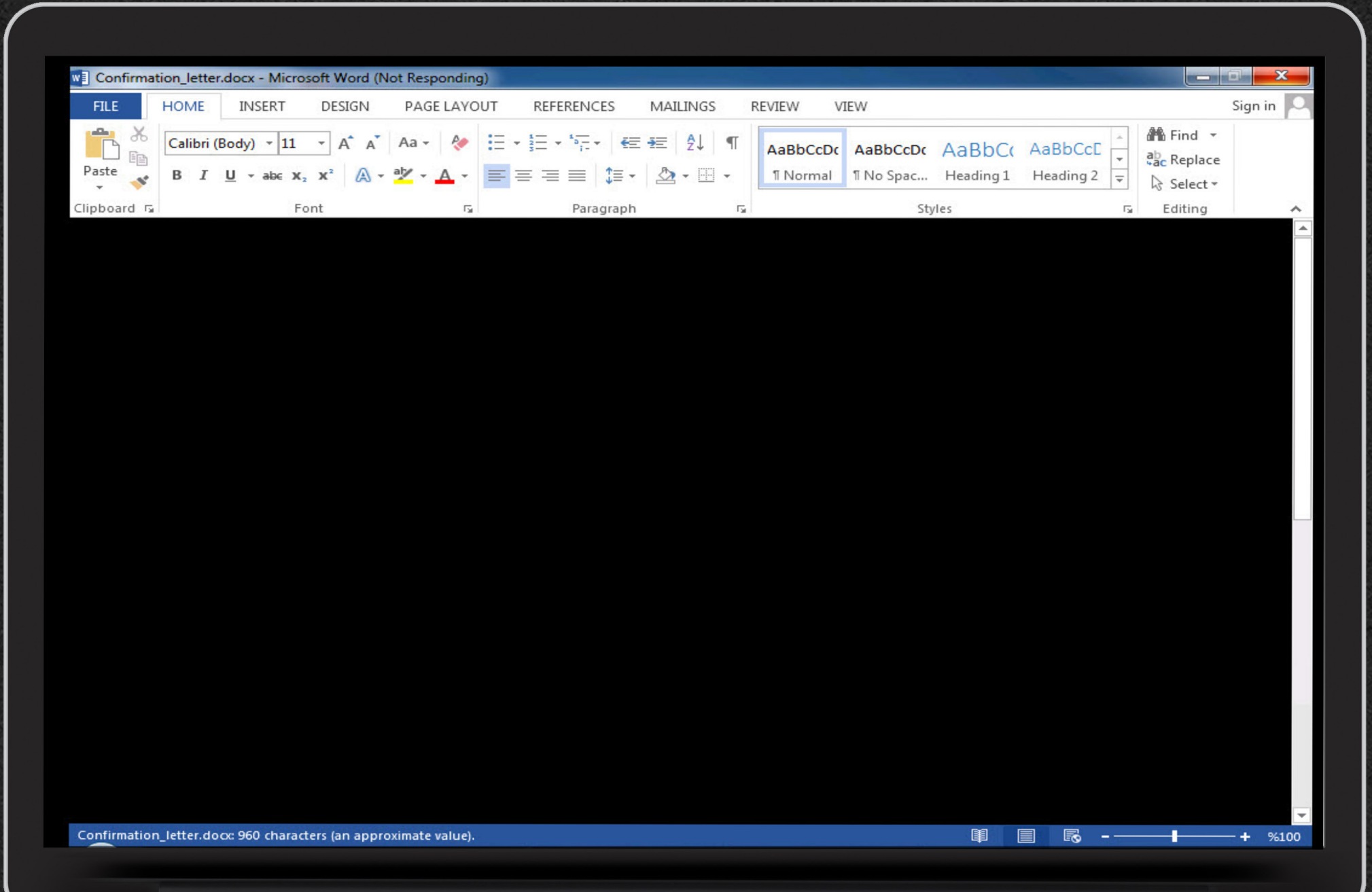
Supporto alle attività connesse agli eventi sismici del 24 agosto 2016: valutazione della vulnerabilità di edifici esistenti e definizione di interventi

See less ^

Assegnista borsa di ricerca PON-METRICS
University of Padua
Jun 2016 - Dec 2016 • 7 mos

See description v

APT GİRİŞİMİ #2



APT GİRİŞİMİ #2

The screenshot shows the Microsoft Word interface with the title bar 'Confirmation_letter.docx - Word (Not Responding)'. The ribbon includes FILE, HOME, INSERT, DESIGN, PAGE LAYOUT, REFERENCES, MAILINGS, REVIEW, and VIEW. The HOME ribbon is active, showing Font, Paragraph, Styles, and Editing groups. The Font group shows Calibri (Body) 11. The Paragraph group shows bulleted and numbered list options. The Styles group shows Normal, No Spac..., Heading 1, and Heading 2. The Editing group shows Find, Replace, and Select options.

On the left, the Document Recovery pane is open, showing 'Available Files' with one file: 'Confirmation_letter.docx - Version created last time t... 01.01.1601 02:00'. A question mark icon and the text 'Which file do I want to save?' are visible at the bottom of the pane, along with a 'Close' button.

The main document content is as follows:

London School of Economics & Political Science
Houghton St, London WC2A 2AE, UK

Confirmation Letter

Dear Sir,

This letter confirms that your candidature was approved for participation in Banking Technology Awards.

Please inform Matteo Salvalaggio on 442039051983 or m.salvalaggio@lse.ac.uk if you need additional information.

Sincerely,

London School of Economics & Political Science, Award Committee

The status bar at the bottom shows 'Confirmation_letter.docx: 960 characters (an approximate value). %100'.

APT GİRİŞİMİ #2

pestudio 8.56 - Malware Initial Assessment - www.winator.com

File Help

c:\users\mert\Desktop\confirmation_letter.docx

- indicators (2/3)
 - virusotal (9/58 - 28.02.2017)**
- abc strings (32/3095)

| engine (58) | positiv (9) | date (dd.mm.y... | age (...) |
|----------------------|-------------------------------|------------------|-----------|
| BitDefender | Exploit.CVE-2015-2545.Gen | 28.02.2017 | 0 |
| Arcabit | Exploit.CVE-2015-2545.Gen | 28.02.2017 | 0 |
| Ad-Aware | Exploit.CVE-2015-2545.Gen | 28.02.2017 | 0 |
| F-Secure | Exploit.CVE-2015-2545.Gen | 28.02.2017 | 0 |
| GData | Exploit.CVE-2015-2545.Gen | 28.02.2017 | 0 |
| Emsisoft | Exploit.CVE-2015-2545.Gen (B) | 28.02.2017 | 0 |
| Kaspersky | HEUR:Exploit.MSWord.Generic | 28.02.2017 | 0 |
| TrendMicro | HEUR_EMBEPS | 28.02.2017 | 0 |
| Bkav | clean | 28.02.2017 | 0 |
| MicroWorld-eScan | clean | 28.02.2017 | 0 |
| nProtect | clean | 28.02.2017 | 0 |
| CMC | clean | 28.02.2017 | 0 |
| CAT-QuickHeal | clean | 28.02.2017 | 0 |
| McAfee | clean | 25.02.2017 | 3 |
| Malwarebytes | clean | 28.02.2017 | 0 |
| VIPRE | clean | 28.02.2017 | 0 |
| SUPERAntiSpyware | clean | 28.02.2017 | 0 |
| TheHacker | clean | 28.02.2017 | 0 |
| K7GW | clean | 28.02.2017 | 0 |
| K7AntiVirus | clean | 28.02.2017 | 0 |
| Baidu | clean | 28.02.2017 | 0 |
| F-Prot | clean | 28.02.2017 | 0 |
| Symantec | clean | 28.02.2017 | 0 |
| ESET-NOD32 | clean | 28.02.2017 | 0 |
| TrendMicro-HouseCall | clean | 28.02.2017 | 0 |
| Avast | clean | 28.02.2017 | 0 |
| ClamAV | clean | 28.02.2017 | 0 |
| Alibaba | clean | 28.02.2017 | 0 |
| NANO-Antivirus | clean | 28.02.2017 | 0 |
| AegisLab | clean | 28.02.2017 | 0 |
| Rising | clean | 28.02.2017 | 0 |
| Comodo | clean | 28.02.2017 | 0 |
| DrWeb | clean | 28.02.2017 | 0 |

APT GİRİŞİMİ #2

TN Microsoft Security Bulletin X

Secure | <https://technet.microsoft.com/en-us/library/security/ms15-099.aspx>

Microsoft Security Bulletin MS15-099 - Critical

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664)

Published: September 8, 2015 | Updated: November 10, 2015

Version: 5.0

Executive Summary

This security update resolves vulnerabilities in Microsoft Office. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who successfully exploited the vulnerabilities could run arbitrary code in the context of the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

This security update is rated Critical for all supported editions of the following software:

- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2013
- Microsoft Office 2013 RT
- Microsoft Office 2016

This security update is rated Important for all supported editions of the following software:

- Microsoft Excel for Mac 2011
- Microsoft Excel 2016 for Mac
- Microsoft SharePoint Foundation 2013, Microsoft SharePoint Server 2013

For more information, see the **Affected Software** section.

The security update addresses the vulnerabilities by correcting how Microsoft Office handles files in memory and by modifying how SharePoint validates web requests. For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see [Microsoft Knowledge Base Article 3089664](#).

Affected Software and Vulnerability Severity Ratings

The following software versions or editions are affected. Versions or editions that are not listed are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, see [Microsoft Support Lifecycle](#).

The following severity ratings assume the potential maximum impact of the vulnerability. For information regarding the likelihood, within 30 days of this security bulletin's release, of the exploitability of the vulnerability in relation to its severity rating and security impact, please see the Exploitability Index in the [September bulletin summary](#).

Microsoft Office Software

MS15-102

MS15-101

MS15-100

MS15-099

MS15-098

MS15-097

MS15-096

MS15-095

MS15-094

MS15-093

MS15-092

MS15-091

MS15-090

MS15-089

MS15-088

MS15-087

MS15-086

MS15-085

MS15-084

MS15-083

MS15-082

MS15-081

Print

Export (0)

Share

On this page

- Executive Summary
- Affected Software and Vulnerability Severity Ratings
- Update FAQ
- Vulnerability Information
- Security Update Deployment
- Acknowledgments
- Disclaimer
- Revisions

IN THIS ARTICLE

- Executive Summary
- Affected Software and Vulnerability Severity Ratings
- Update FAQ
- Vulnerability Information
- Security Update Deployment
- Acknowledgments
- Disclaimer
- Revisions

APT GİRİŞİMİ #2

FireEye™ Dashboard | ALERTS | Settings | Reports | About

Alerts | Summaries | Filters

| | | | | | | |
|----------------|---------|------|------------------|-------------------|---------------------------------|---------|
| Malware Object | 1046004 | docx | Exploit.docx.MVX | 02/28/17 19:53:10 | 2abe3cc4bf46455a945d56c27e9fb45 | 579.140 |
|----------------|---------|------|------------------|-------------------|---------------------------------|---------|

Malware: **Exploit.docx.MVX**
Application Type: Multiple MS Word X
File Type: docx

VM Capture: pcap 976 bytes (text)
Raw Alert: Download (xml)
Victim IP:
Src MAC Address: 00:09:0f:09:0d:0b
Dst MAC Address: 00:50:56:a6:2e:df
MD5: 2abe3cc4bf46455a945d56c27e9fb45
Analysis OS: Microsoft Windows7 32-bit 6.1.sp1.16.0901
Archived Object: 680817e04622e8270f3c70c2e842124d.zip

[Suppress This Alert](#)

Download Source Headers

| | | | | |
|---------------------------|--|----------|------------------|-------------------------------|
| GET | http://www.mertsarica.com/ | HTTP/1.1 | X-RBT-SCAR | |
| Accept | text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 | | HTTP | 1.1 200 OK |
| Accept-Language | en-US,en;q=0.8 | | Date | Tue, 28 Feb 2017 16:47:39 GMT |
| Cookie | __cfduid=d57c03f25aac07d0478061f8a169cd4051488300428 | | Etag | "58b5a99b-3ce9d" |
| Host | www.mertsarica.com | | CF-RAY | 33855c10d476149d-AMS |
| Proxy-Authorization | NTLM TIRMTVNTUADAAAAGAAAYHAYAAAAABgA1gAAAAvADABAAAAADAAAEwAAAAeAB4AWAAA AAAAAACmAAAAABYKBAEYASQBOAEEATgBTAFAQAMQA3ADIAOQA4AEKAQgBHAFCVQAZADUAMQAw ADEEAMAAvADMANA1AL0xAdvrMqMn6YkxMDgzHafmDc9EJJoDytN53zcz+eP3MUQTY2yeW6+pdNS zzQ668A== | | Server | cloudflare-nginx |
| Proxy-Connection | keep-alive | | Content-Type | application/zip |
| RVBD-CSH | | | Accept-Ranges | bytes |
| RVBD-SSH | | | Last-Modified | Tue, 28 Feb 2017 16:47:23 GMT |
| Upgrade-Insecure-Requests | 1 | | Content-Length | 249501 |
| User-Agent | Mozilla/4.0 (compatible; MSIE 5.5; Windows 98) | | Proxy-Connection | Keep-Alive |
| X-RBT-Optimized-By | rvbprdbt03 (RIOS 9.5.0) SC | | | |

OS Change Detail (version: 1.2712) | Items: 88 | OS Info: Microsoft Windows7 32-bit 6.1.sp1.16.0901 [Top](#)

| Type | Mode/Class | Details (Path/Message/Protocol/Hostname/Qtype/ListenPort etc.) | Process ID | Parent ID | File Size |
|---------------|------------|--|------------|-----------|-----------|
| Analysis | Malware | | | | |
| Application | | | | | |
| Os | | Name: windows Version: 6.1.7601 Service Pack: 1 Arch: x86 | | | |
| Os Monitor | | Version: 16R1 Build: 519813 Date: Aug 31 2016 Time: 18:44:00 | | | |
| Config Update | | | | | |
| Uac | Service | Portable Device Enumerator Service | | | |
| Uac | Service | Background Intelligent Transfer Service | | | |
| Uac | Service | Software Protection | | | |
| Uac | Service | Security Center | | | |

APT GİRİŞİMİ #2

pestudio 8.56 - Malware Initial Assessment - www.winator.com

File Help

c:\users\mert\Desktop\decoded_malw

| | type | size | location | blacklisted (200) | item (1300) |
|-----------------------------|-------|------|----------|-------------------|--|
| indicators (3/14) | ascii | 4 | - | - | <Lt0 |
| virustotal (n/a) | ascii | 4 | - | - | \$rFB |
| dos-stub (64 bytes) | ascii | 4 | - | - | \$fB |
| file-header (20 bytes) | ascii | 17 | - | - | function powercat |
| optional-header (224 bytes) | ascii | 8 | - | - | param(|
| directories (2) | ascii | 35 | - | - | [alias("Client")][string]\$c="", |
| sections (4) | ascii | 39 | - | - | [alias("Listen")][switch]\$l=\$False, |
| libraries (2/8) | ascii | 57 | - | - | [alias("Port")][Parameter(Position=-1)][string]\$p="", |
| imports (161) | ascii | 36 | - | - | [alias("Execute")][string]\$e="", |
| exports (n/a) | ascii | 51 | - | - | [alias("ExecutePowershell")][switch]\$ep=\$False, |
| exceptions (n/a) | ascii | 34 | - | - | [alias("Relay")][string]\$r="", |
| tls-callbacks (n/a) | ascii | 36 | - | - | [alias("UDP")][switch]\$u=\$False, |
| resources (n/a) | ascii | 38 | - | - | [alias("dnscat2")][string]\$dns="", |
| strings (200/1300) | ascii | 51 | - | - | [alias("DNSFailureThreshold")][int32]\$dnsft=10, |
| debug (n/a) | ascii | 35 | - | - | [alias("Timeout")][int32]\$t=60, |
| manifest (n/a) | ascii | 65 | - | - | [Parameter(ValueFromPipeline=\$True)][alias("Input")]\$i=\$Null, |
| file-version (n/a) | ascii | 83 | - | - | [ValidateSet('Host', 'Bytes', 'String')][alias("OutputType")][string]\$o="Host", |
| certificate (n/a) | ascii | 40 | - | - | [alias("OutputFile")][string]\$of="", |
| overlay (n/a) | ascii | 43 | - | - | [alias("Disconnect")][switch]\$d=\$False, |
| | ascii | 43 | - | - | [alias("Repeater")][switch]\$rep=\$False, |
| | ascii | 48 | - | - | [alias("GeneratePayload")][switch]\$g=\$False, |
| | ascii | 49 | - | - | [alias("GenerateEncoded")][switch]\$ge=\$False, |
| | ascii | 36 | - | - | [alias("Help")][switch]\$h=\$False |
| | ascii | 38 | - | - | ##### HELP ##### |
| | ascii | 11 | - | - | \$Help = " |
| | ascii | 41 | - | - | powercat - Netcat, The Powershell Version |
| | ascii | 58 | - | - | Github Repository: https://github.com/besimorhino/powercat |
| | ascii | 72 | - | - | This script attempts to implement the features of netcat in a powershell |
| | ascii | 72 | - | - | script. It also contains extra features such as built-in relays, execute |
| | ascii | 33 | - | - | powershell, and a dnscat2 client. |
| | ascii | 46 | - | - | Usage: powercat [-c or -l] [-p port] [options] |
| | ascii | 83 | - | - | -c <ip> Client Mode. Provide the IP of the system you wish to connect to. |
| | ascii | 83 | - | - | If you are using -dns, specify the DNS Server to send queries to. |

APT GİRİŞİMİ #2

pestudio 8.56 - Malware Initial Assessment - www.winitor.com

File Help

c:\users\mert\Desktop\decoded_malv

| | type | size | location | blacklisted (200) | item (1300) |
|-----------------------------|---------|------|----------|-------------------|--------------------------------------|
| indicators (3/14) | unicode | 15 | - | - | UninstallString |
| virustotal (n/a) | unicode | 14 | - | - | DisplayVersion |
| dos-stub (64 bytes) | unicode | 9 | - | - | Publisher |
| file-header (20 bytes) | unicode | 20 | - | - | QuietUninstallString |
| optional-header (224 bytes) | unicode | 27 | - | - | %2d/%.2d/%d %.2d:%.2d:%.2d |
| directories (2) | unicode | 28 | - | - | L d/%. d/%d %.2d:%.2d:%.2d |
| sections (4) | unicode | 5 | - | - | % |
| libraries (2/8) | unicode | 13 | - | - | InternetProxy |
| imports (161) | unicode | 8 | - | - | %d:%s%; |
| exports (n/a) | unicode | 15 | - | - | \%u:%d64u:%s%; |
| exceptions (n/a) | unicode | 5 | - | - | %s/%s |
| tls-callbacks (n/a) | unicode | 5 | - | - | %s%s\ |
| resources (n/a) | unicode | 4 | - | - | %s%s |
| strings (200/1300) | unicode | 5 | - | - | %S:%u |
| debug (n/a) | unicode | 5 | - | - | %S:%d |
| manifest (n/a) | unicode | 36 | - | - | [%s] - [%.2d/%.2d/%d %.2d:%.2d:%.2d] |
| file-version (n/a) | unicode | 11 | - | - | {Backspace} |
| certificate (n/a) | unicode | 8 | - | - | {Return} |
| overlay (n/a) | unicode | 5 | - | - | {Tab} |
| | unicode | 12 | - | - | {Arrow Left} |
| | unicode | 10 | - | - | {Arrow Up} |
| | unicode | 13 | - | - | {Arrow Right} |
| | unicode | 12 | - | - | {Arrow Down} |
| | unicode | 6 | - | - | {Home} |
| | unicode | 9 | - | - | {Page Up} |
| | unicode | 11 | - | - | {Page Down} |
| | unicode | 5 | - | - | {End} |
| | unicode | 7 | - | - | {Break} |
| | unicode | 8 | - | - | {Delete} |
| | unicode | 8 | - | - | {Insert} |
| | unicode | 14 | - | - | {Print Screen} |
| | unicode | 13 | - | - | {Scroll Lock} |
| | unicode | 11 | - | - | {Caps Lock} |
| | unicode | 5 | - | - | {Alt} |
| | unicode | 5 | - | - | {Esc} |
| | unicode | 9 | - | - | {Ctrl+%c} |
| | unicode | 4 | - | - | {%s} |
| | unicode | 4 | - | - | %.2X |
| | unicode | 5 | - | - | %s\%s |

APT GİRİŞİMİ #2

pestudio 8.56 - Malware Initial Assessment - www.winitor.com

File Help

c:\users\mert\Desktop\decoded_malware\oglgcache.exe

| type | size | location | blacklisted (200) | item (1300) |
|-------|------|----------|-------------------|---|
| ascii | 4 | - | x | \$.VB |
| ascii | 52 | - | x | powercat -c 10.1.1.1 -p 53 -dns c2.example.com |
| ascii | 59 | - | x | powercat -l -p 8000 -r dns:10.1.1.153:c2.example.com |
| ascii | 165 | - | x | cmd.exe /c powershell; Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process -Force... |
| ascii | 8 | - | x | %WINDIR% |
| ascii | 19 | - | x | %system32%\cmd.exe |
| ascii | 18 | - | x | checkip.dyndns.org |
| ascii | 24 | - | x | Host: checkip.dyndns.org |
| ascii | 80 | - | x | User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko |
| ascii | 82 | - | x | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 |
| ascii | 31 | - | x | Accept-Language: en-US,en;q=0.8 |
| ascii | 6 | - | x | %TEMP% |
| ascii | 40 | - | x | 84.200.2.12:443; |
| ascii | 16 | - | x | %TEMP%\loopc.cmd |
| ascii | 27 | - | x | C:\Windows\system32\cmd.exe |
| ascii | 9 | - | x | psapi.dll |
| ascii | 19 | - | x | GetModuleFileNameEx |
| ascii | 6 | - | x | ns.exe |
| ascii | 6 | - | x | System |
| ascii | 23 | - | x | SetThreadExecutionState |
| ascii | 27 | - | x | C:\Windows\system32\cmd.exe |
| ascii | 46 | - | x | SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ |
| ascii | 56 | - | x | SOFTWARE\Microsoft\Active Setup\Installed Components\%s\ |
| ascii | 11 | - | x | Secur32.dll |
| ascii | 22 | - | x | LsaGetLogonSessionData |
| ascii | 25 | - | x | LsaEnumerateLogonSessions |
| ascii | 9 | - | x | psapi.dll |
| ascii | 19 | - | x | GetModuleFileNameEx |
| ascii | 12 | - | x | ERNEL32.DLL |
| ascii | 11 | - | x | winhttp.dll |
| ascii | 11 | - | x | WinHttpOpen |
| ascii | 21 | - | x | WinHttpGetProxyForUrl |
| ascii | 18 | - | x | WinHttpCloseHandle |
| ascii | 37 | - | x | WinHttpGetIEProxyConfigForCurrentUser |
| ascii | 19 | - | x | GetNativeSystemInfo |
| ascii | 11 | - | x | ProductType |
| ascii | 47 | - | x | SYSTEM\CurrentControlSet\Control\ProductOptions |
| ascii | 5 | - | x | WINNT |
| ascii | 8 | - | x | LANMANNT |

APT GİRİŞİMİ #2

Search | FireEye - MySIGHT

Secure | <https://mysight.isightpartners.com/search/index/index?search-type=basic&contains=84.200.2.12&include-sensitive=0&taglist-0=ASN&page=1&size=25>

QNB Finansbank | ISIGHT INTELLIGENCE MySIGHT | Intel by Role | Intel by Category | Support

84.200.2.12

SEARCH TERM(S)
84.200.2.12

Advanced | Any date | Role | Category | Written for anyone | Intelligence Type | Report Type | Risk Rating

SEARCH RESULTS

| Title | Date | Report ID | Category | Role | Version |
|--|--------------------|-------------|-------------------|-------------|---------|
| + CVE-2017-0261 Used as Zero-Day by Turla Group and Unidentified Group Targeting Banks | May 9, 2017 12:52 | 17-00004695 | CC CE | FS | 1 |
| + FireEye Labs Research: EPS Processing Zero-Days Exploited by Multiple Threat Actors | May 10, 2017 11:05 | 17-00004542 | CI CC CE EN HK VE | EX FS OP VU | 1 |

Showing 1-2 of 2 reports | 25 per page

Home | Intel by Role | Intel by Category | Support | My Account

Search | Operational | Cyber Espionage | Tech Support | My Delivery Profiles

My Saved Searches | Fusion | Hactivism | FAQ | Learn More About FireEye

Executive | Enterprise | Technical Product Documentation

Vulnerability | Critical Infrastructure | Contact Us

Cyber Crime

Vulnerability and Exploitation

©2007-2017 FireEye, Inc. All Rights reserved. | [Terms of Use](#)

This application and its contents are the property of FireEye, Inc. and are protected by all applicable laws and subject to subscription terms, applicable EULAs and other contractual agreements with our clients. Unauthorized use may result in legal action.

(v1.3.1.241)

APT GİRİŞİMİ #2

Report 17-00004695 | FireEye

Secure | <https://mysight.isightpartners.com/report/full/17-00004695>

QNB FİNANSBANK | ISIGHT INTELLIGENCE MySIGHT | Intel by Role | Intel by Category | Support | Quick search...

FireEye THREAT INTELLIGENCE

Fusion (FS) | Cyber Crime (CC) | **Cyber Espionage (CE)**

CVE-2017-0261 Used as Zero-Day by Turla Group and Unidentified Group Targeting Banks

17-00004695 CC CE
May 09, 2017 12:52:00 PM, Version:1

Indicators PDF Print

EXECUTIVE SUMMARY

- CVE-2017-0261 is an EPS vulnerability in Microsoft Office that allows remote code execution. This vulnerability was patched by Microsoft on May 9.
- A document exploiting this vulnerability was used by Turla Group to deliver a SHIRME payload to a European diplomatic entity.
- The same vulnerability was used to distribute a NetWire payload to the Middle Eastern offices of regional and global banks.

DETAILS TECHNICAL TABS ON

CVE-2017-0261, patched on May 9, 2017, is a vulnerability in how Microsoft Office handles EPS files. Successful exploitation allows attackers to execute arbitrary code. This vulnerability was first known to be exploited in the wild in late February 2017 and has been exploited by multiple groups with different motivations.

- Further discussion of the mechanics behind CVE-2017-0261 is available from FireEye Labs [here](#).
- This vulnerability was first observed being exploited by an unknown, likely financially motivated actor. Documents that exploited CVE-2017-0261 to deliver a NETWIRE payload were distributed to multiple banks located in the Middle East.
- Turla Group used a CVE-2017-0261 document to deliver a SHIRME payload to a European diplomatic entity.

Unknown Actor Targets Middle Eastern Banks

Related Reports 5

- [Turla Team Targets Indian Government with KOPILUWAK via Spear-Phishing Attempt \(17-00007466\)](#)
- [NetWire Malware Overview \(16-00017874\)](#)
- [Industry Brief: Aviation \(17-00006525\)](#)
- [APT28 Using New XTUNNEL Variant in Likely Intrusion Against Republic of Georgia Government \(17-00007148\)](#)
- [TEMP.Hermit Targets Multiple U.S. Aerospace Defense Contractors \(17-00007434\)](#)

“Zeki insanları alıp sonra onlara ne yapacaklarını söylemek mantıklı gelmiyor.
Biz zeki insanları işe alırsak ki onlar bize ne yapacağımızı söylesinler.”

Steve Jobs

SONUÇ.

Kum havuzu teknolojilerine yatırım yapmak için hala çok geç değil. (FireEye NX vb.)

Her kurum hacklenebilir bu nedenle Bilgisayar Olayları Tespit (EDR) sistemleri de muhakkak kullanılmalıdır. (FireEye HX vb.)

Günün sonunda kurumunuzu kurtaracak olanlar insanlardır, çalışanlarınıza ve uzmanlaşmaya yatırım yapın. :)



NOTLAR.

Bu sunuma konu olan ilk APT girişimini blogumda okuyabilirsiniz. ([Bir APT Girişimi](#))

Bu sunuma konu olan ikinci APT girişimini ise [2 Ekim](#)'de blogumda okuyabilirsiniz.
([Yakından da Yakın](#))

Bloguma konu olan yazılara, ürünleri ile haberleri olmadan katkıda buldukları için [FireEye](#) firmasına teşekkür ederim. :)



SORULAR?



MUTLU SON.

 mertsarica  mertsarica

mertsarica@gmail.com



Sumum Tasarım

MINIMALISTA
C R E A T I V E A G E N C Y

Nuvo Dragos A Blok D: 7 T: 0216 340 21 26



minimalista.com.tr



[minimalistacreative](https://www.facebook.com/minimalistacreative)



[minimalista_creative](https://www.instagram.com/minimalista_creative)

