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 Kolleksiyoncusu — CISSP , SSCP , OSCP , OPST , CREA, CEREA

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

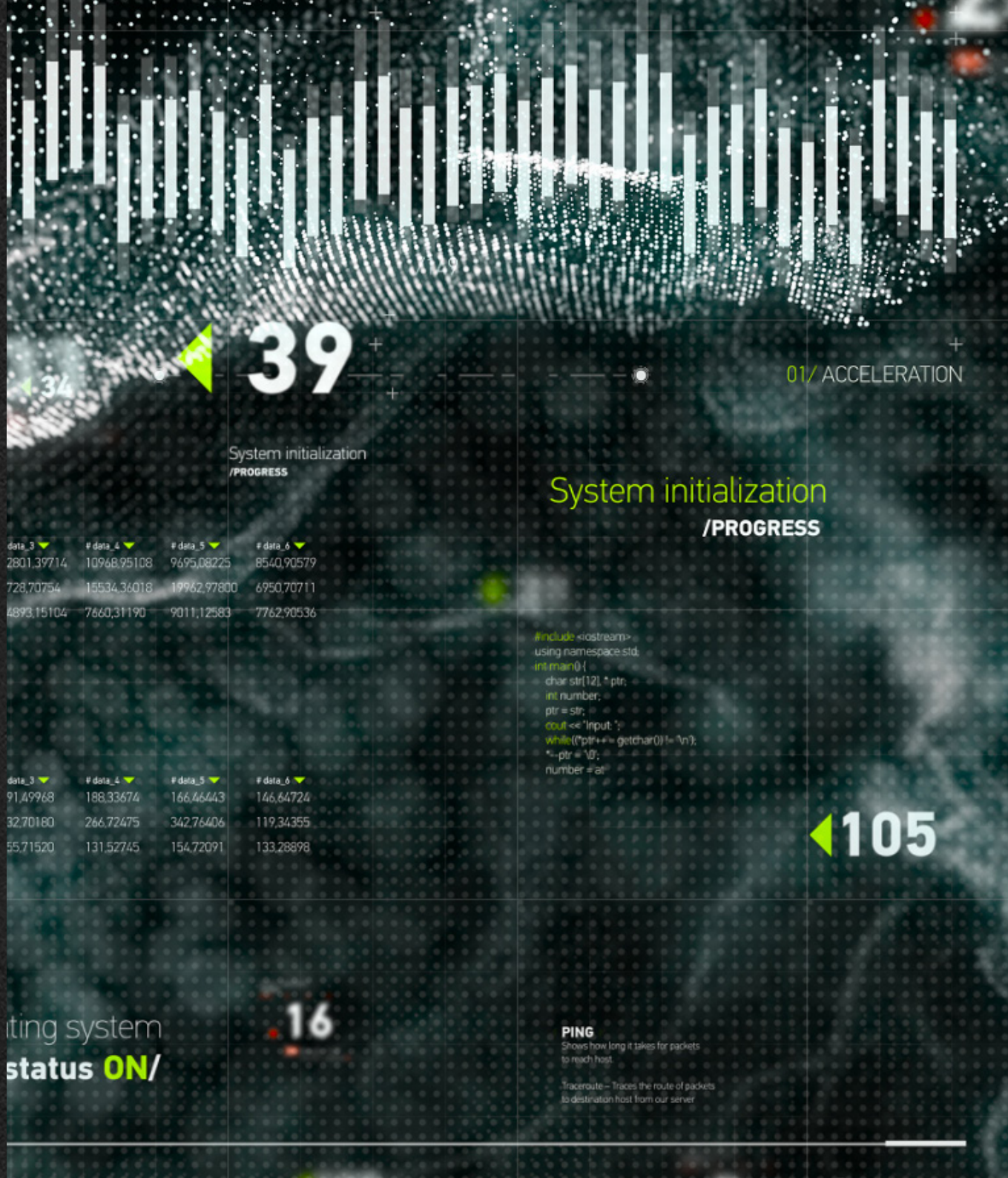
APT NEDİR ?

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 eğitimli 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'ın 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

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,

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,

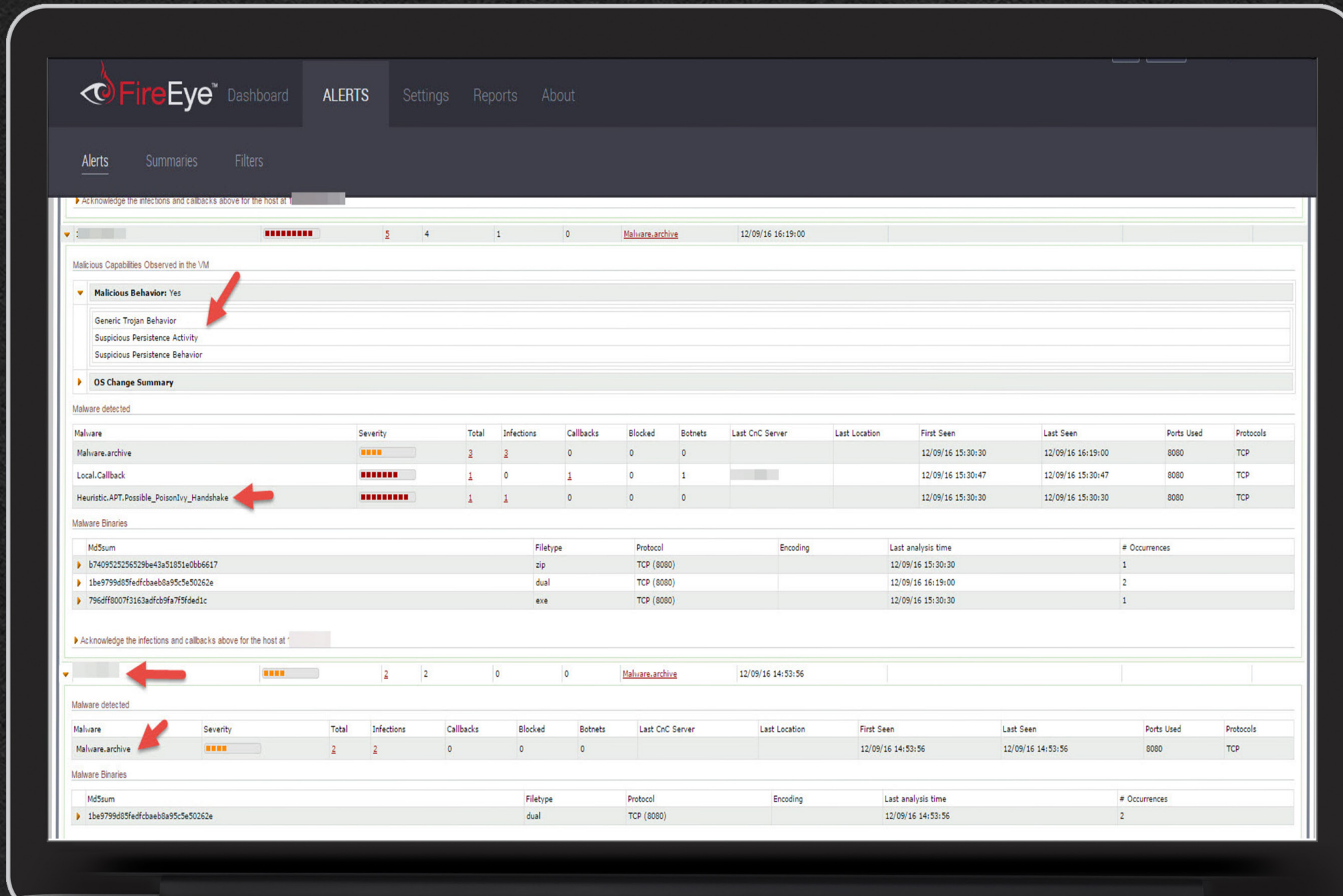
APT GİRİŞİMİ #1

Foremost, you have to fill out and send me the Expert application form:
http://moya.bus.miami.edu/~emil/Documents/Application_Form.doc

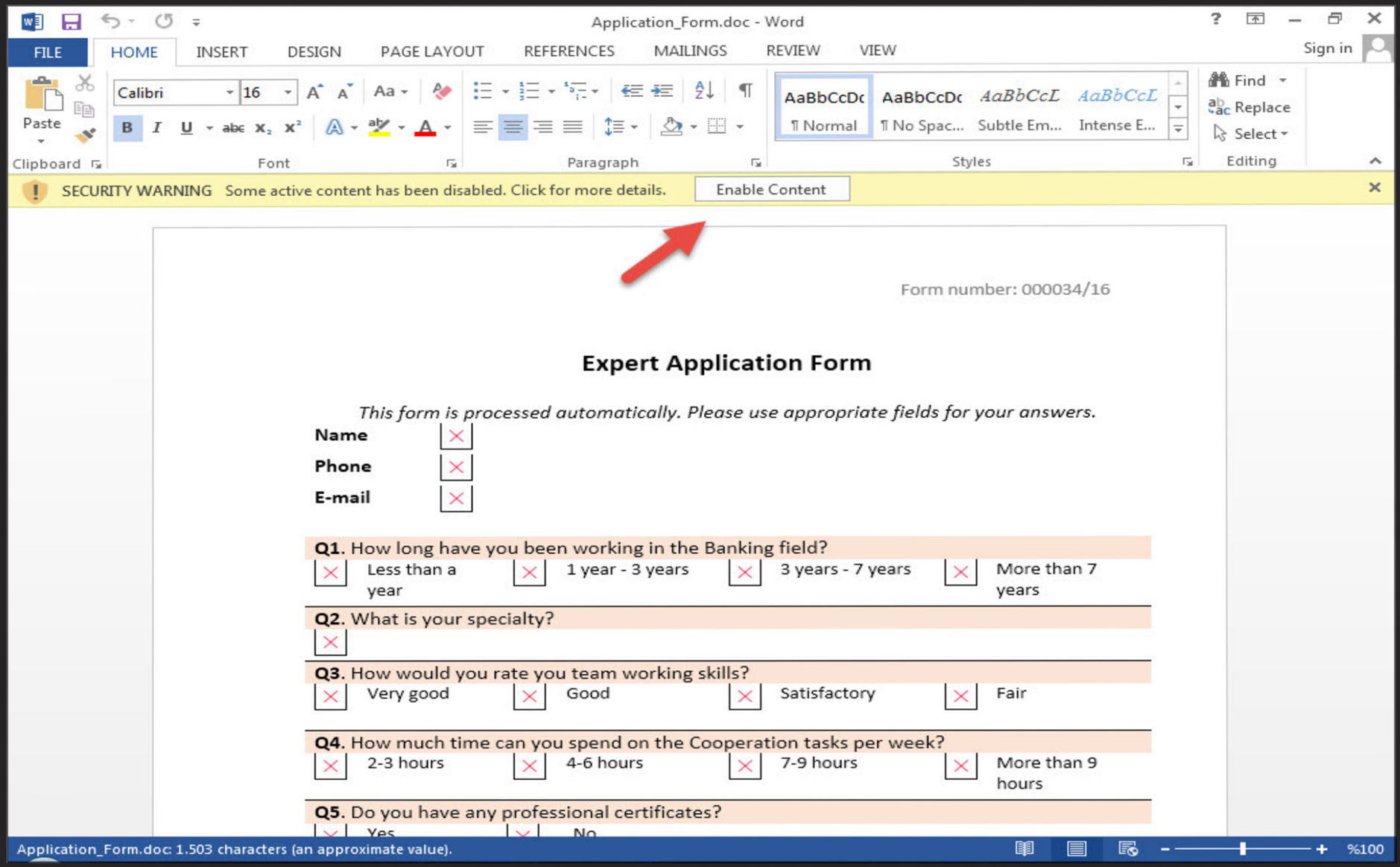
Further, I will prepare the NDA. After that, I will send you first questions.

Best,

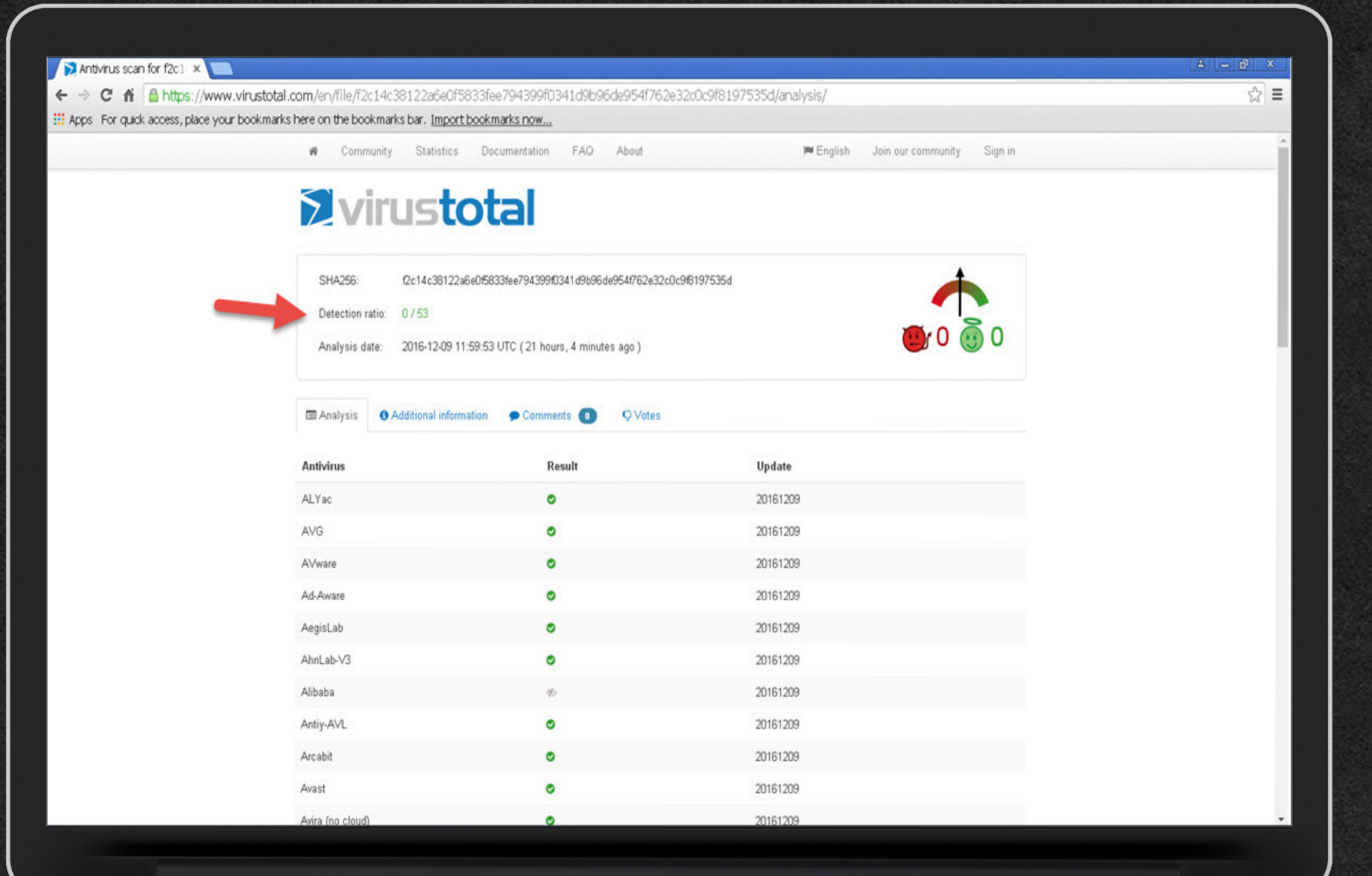
APT GİRİŞİMİ #1



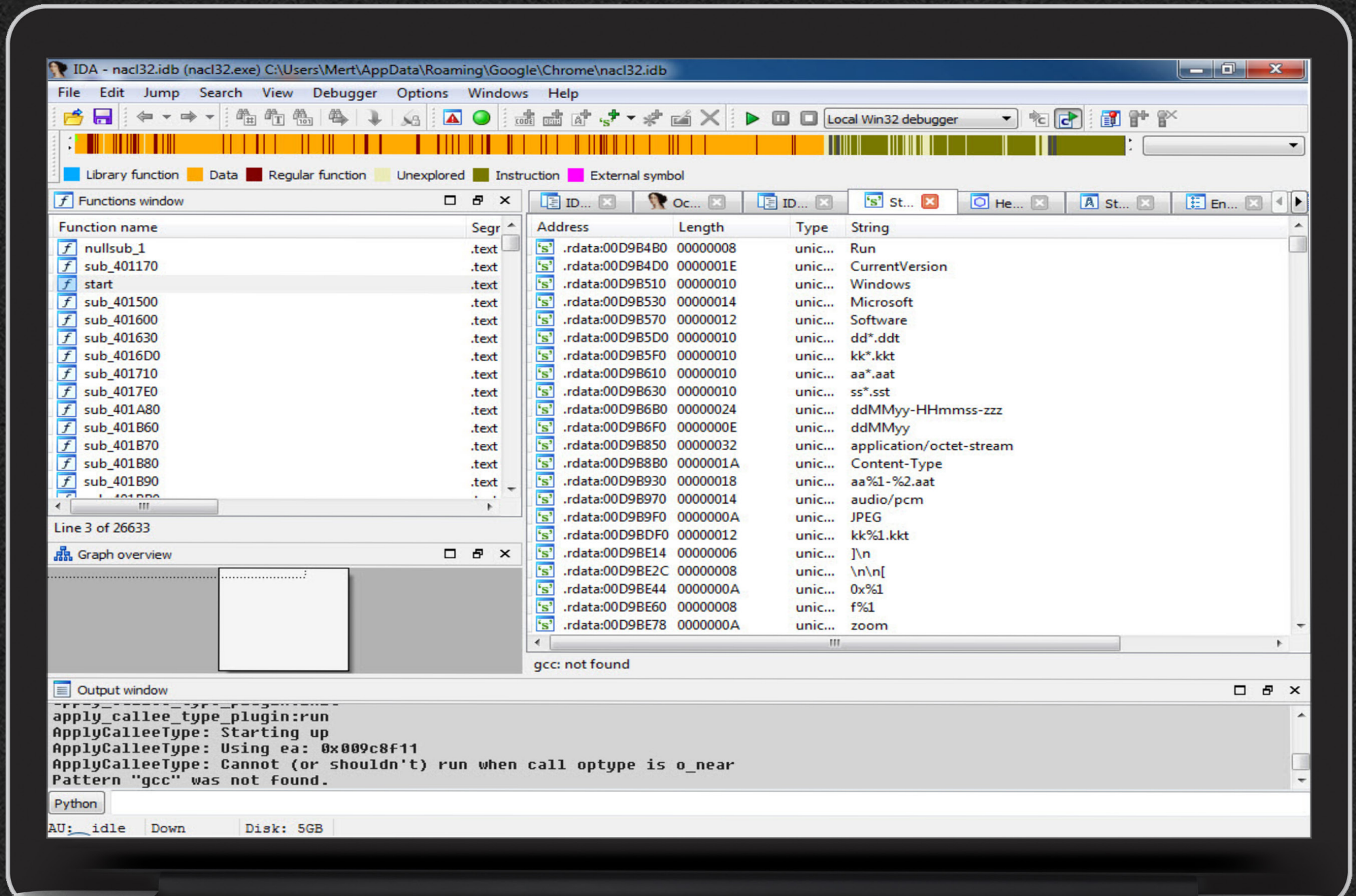
APT GİRİŞİMİ #1



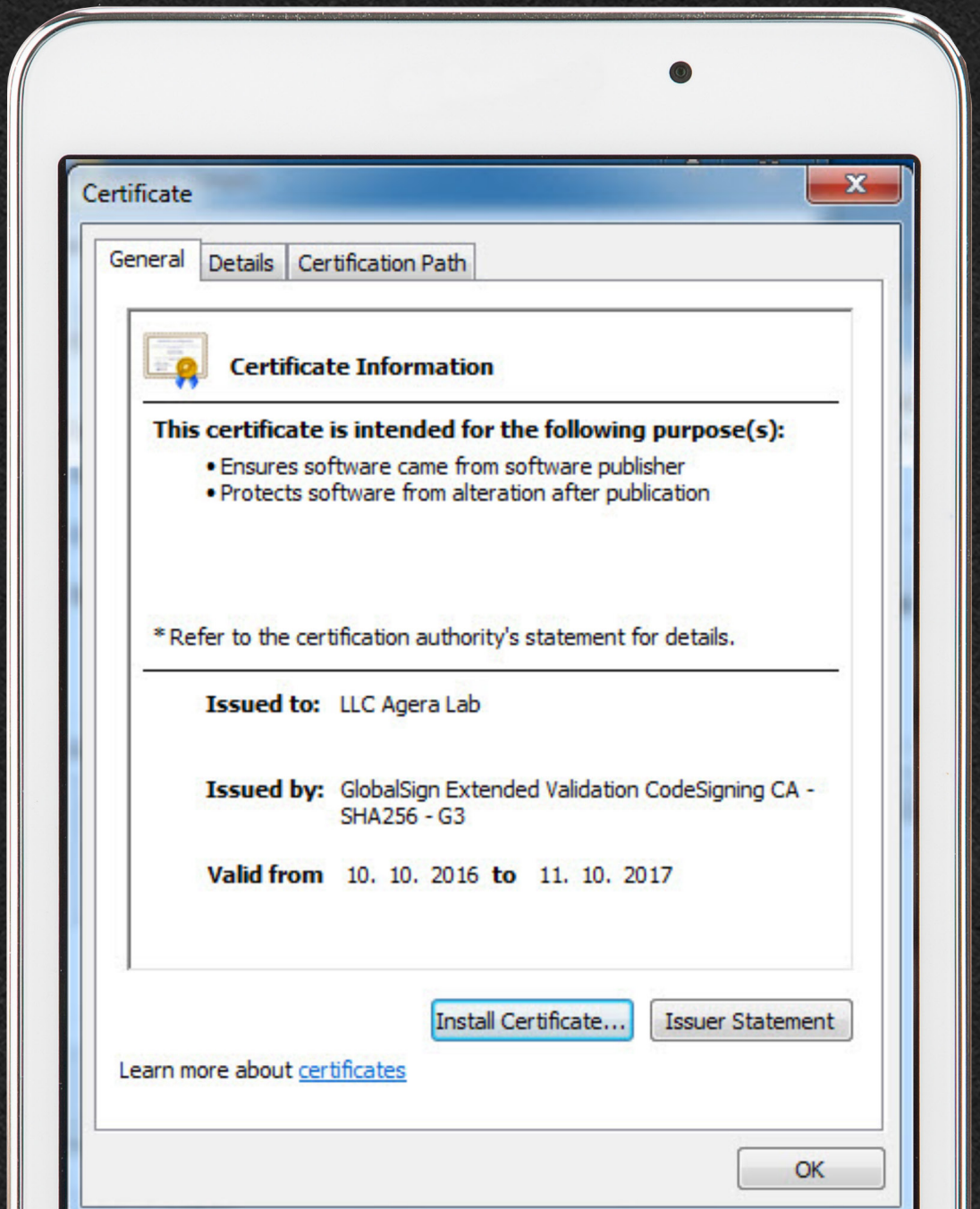
APT GİRİŞİMİ #1



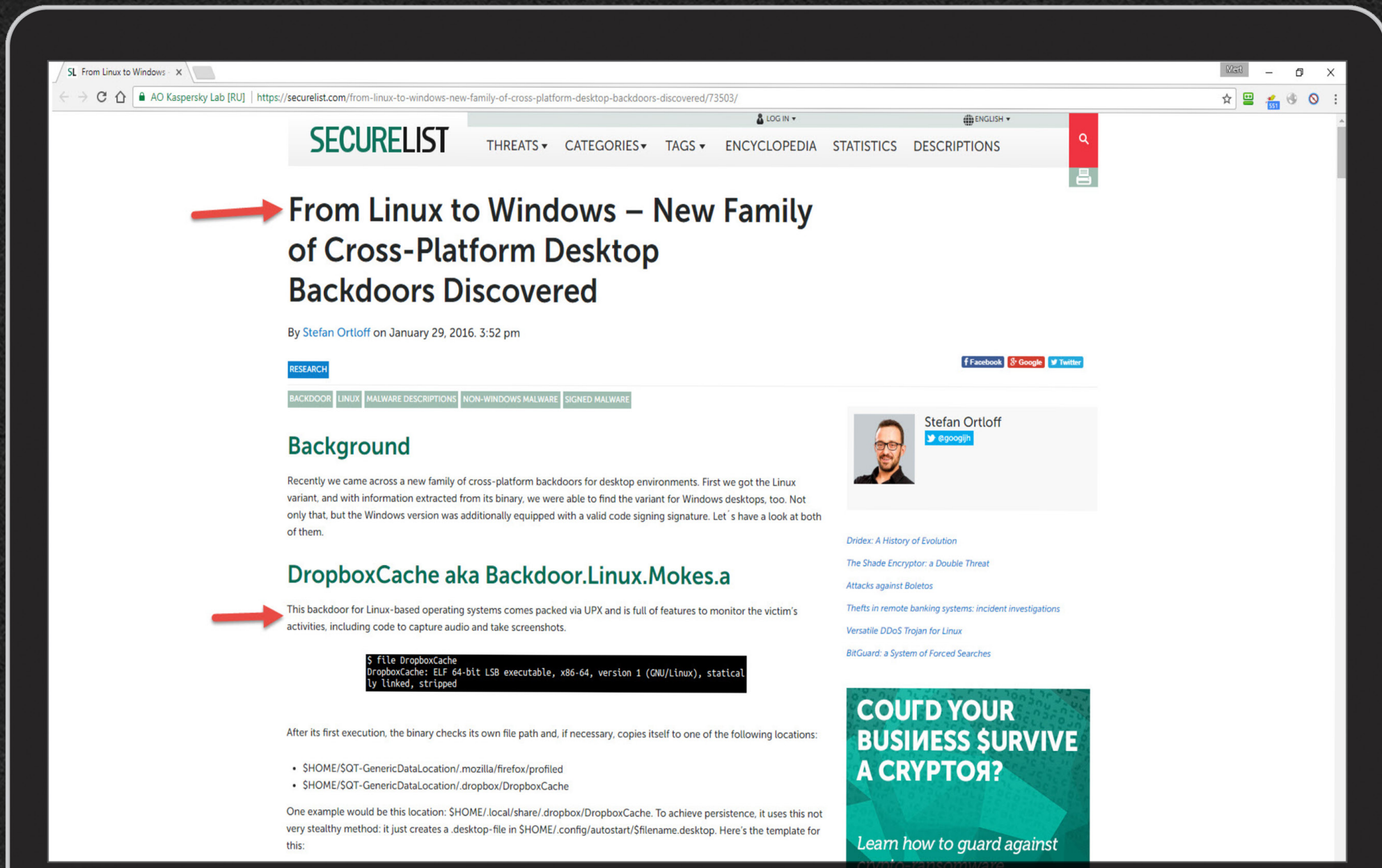
APT GİRİŞİMİ #1



APT GİRİŞİMİ #1



APT GİRİŞİMİ #1



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.

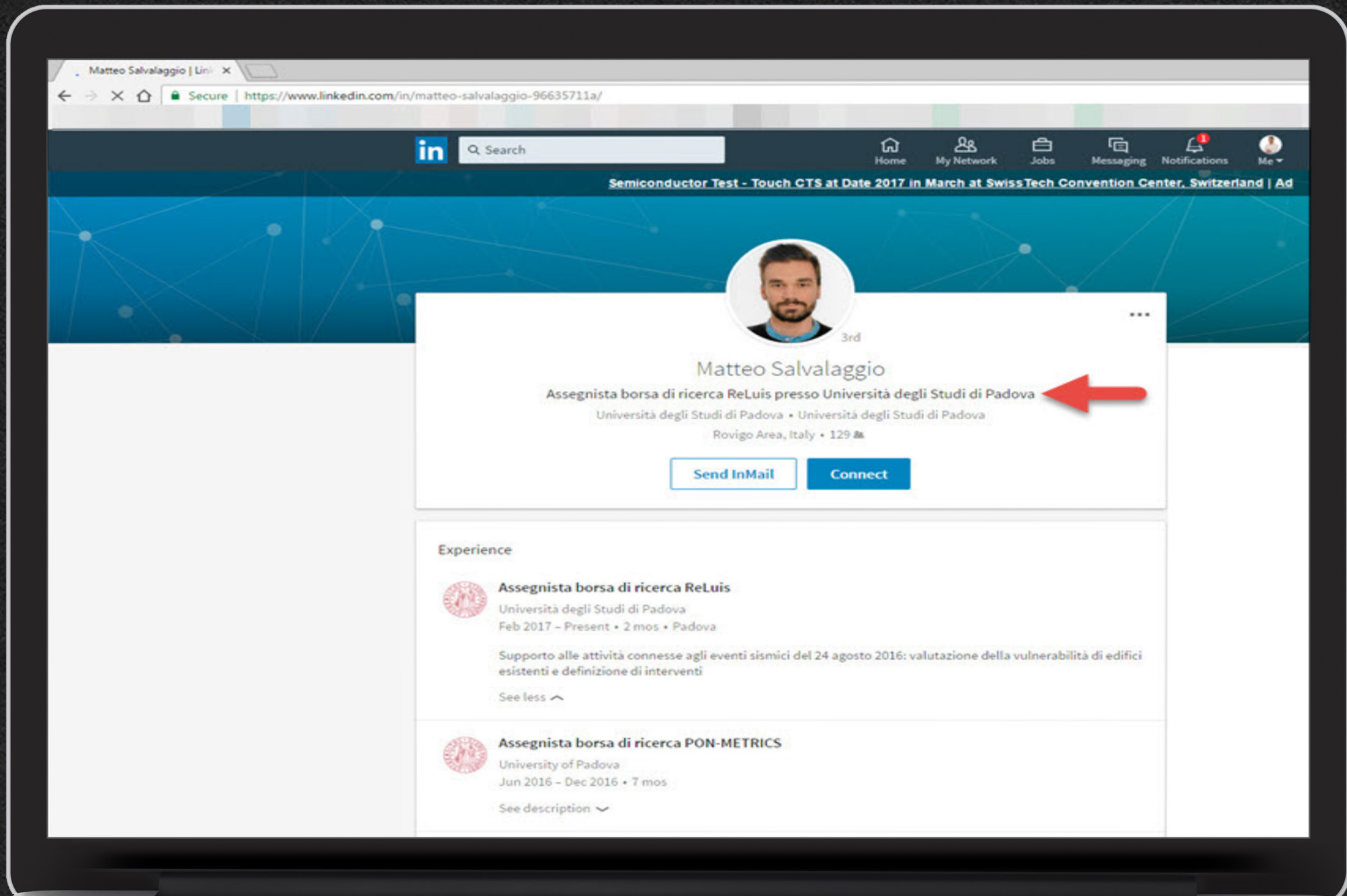
The attachment contains the copy of the confirmation letter. Please pay attention to the expiry period of the certificate. You will get the hard copy via mail within 2 weeks.

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

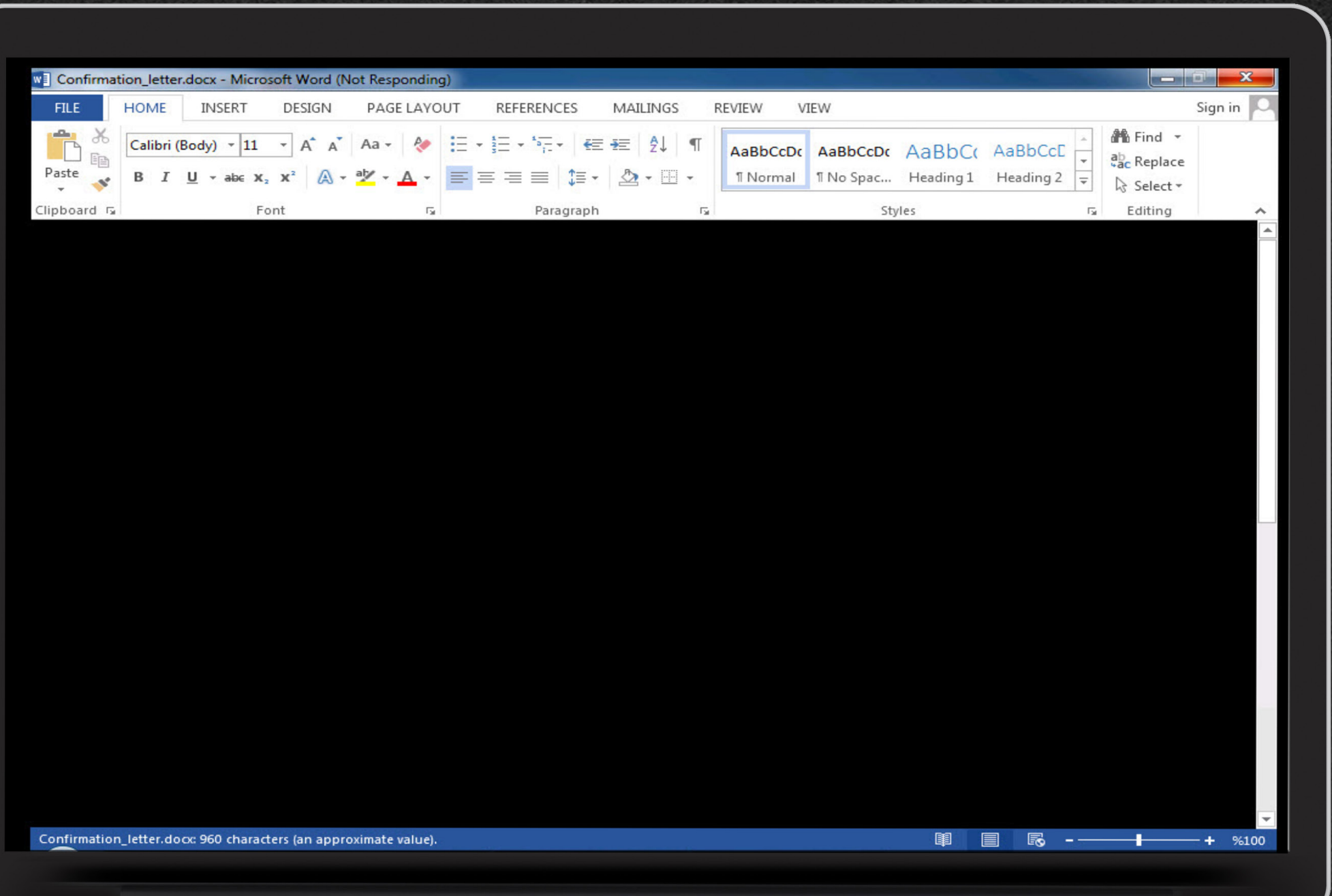
Best regards,
Matteo

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

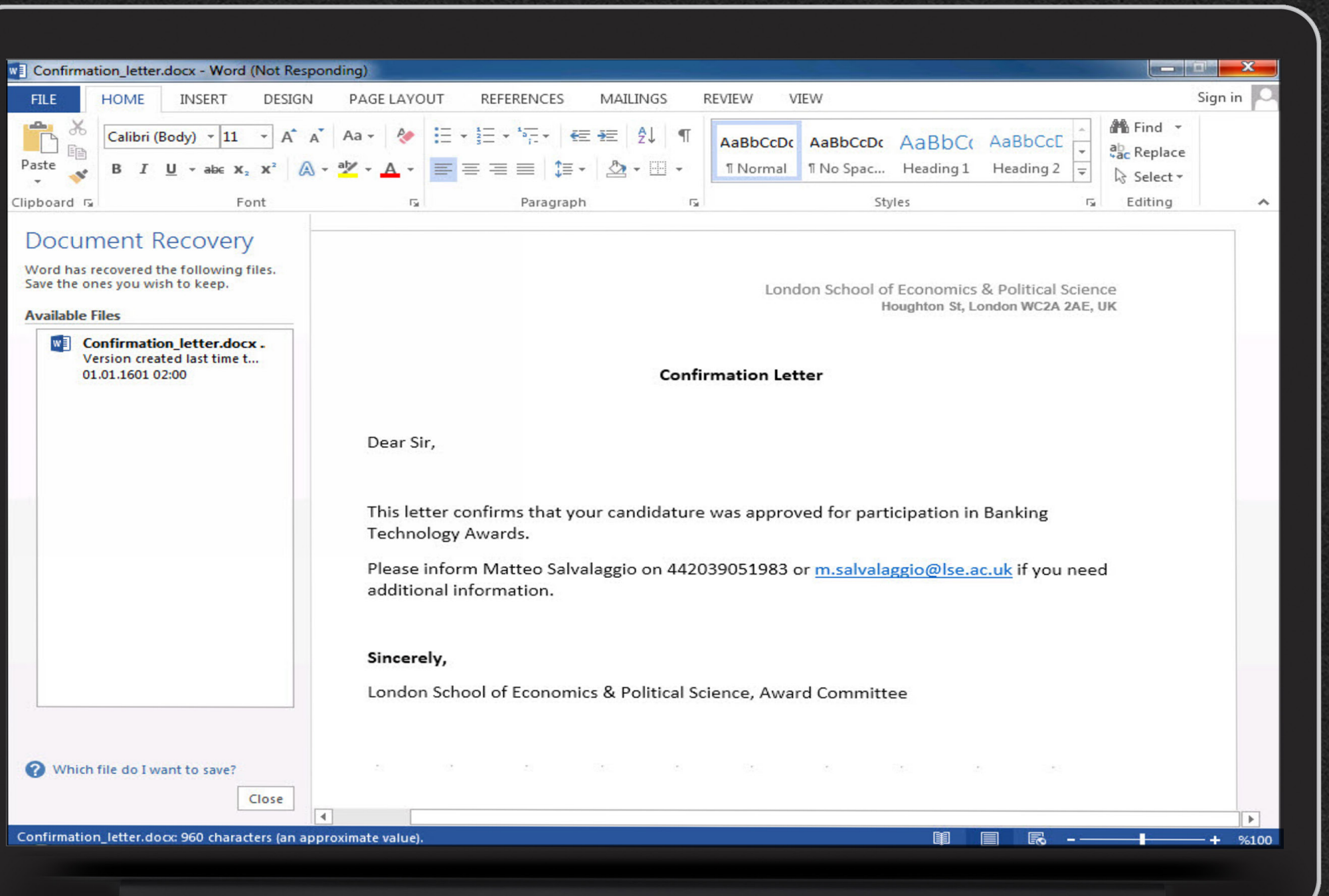
APT GİRİŞİMİ #2



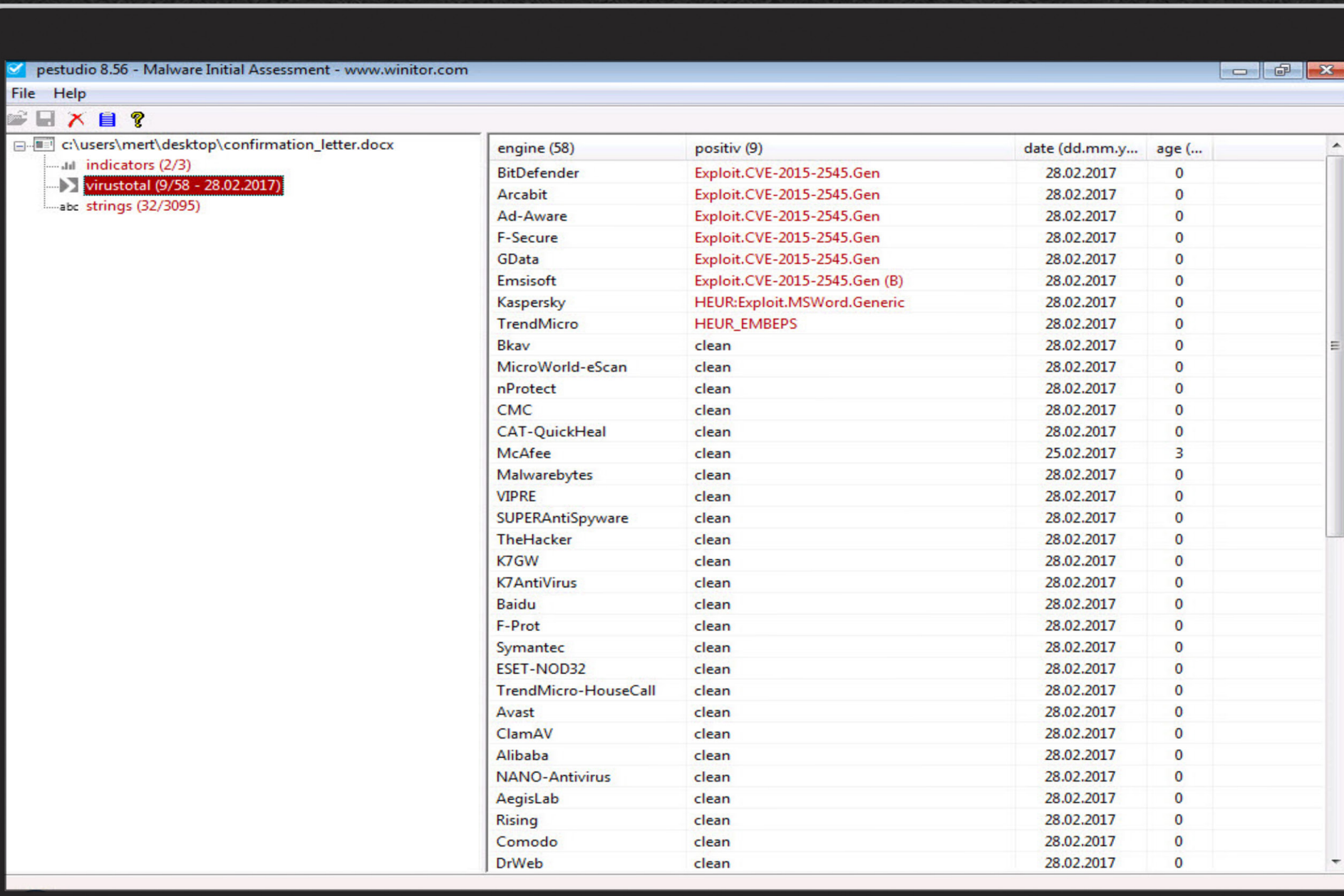
APT GİRİŞİMİ #2



APT GİRİŞİMİ #2

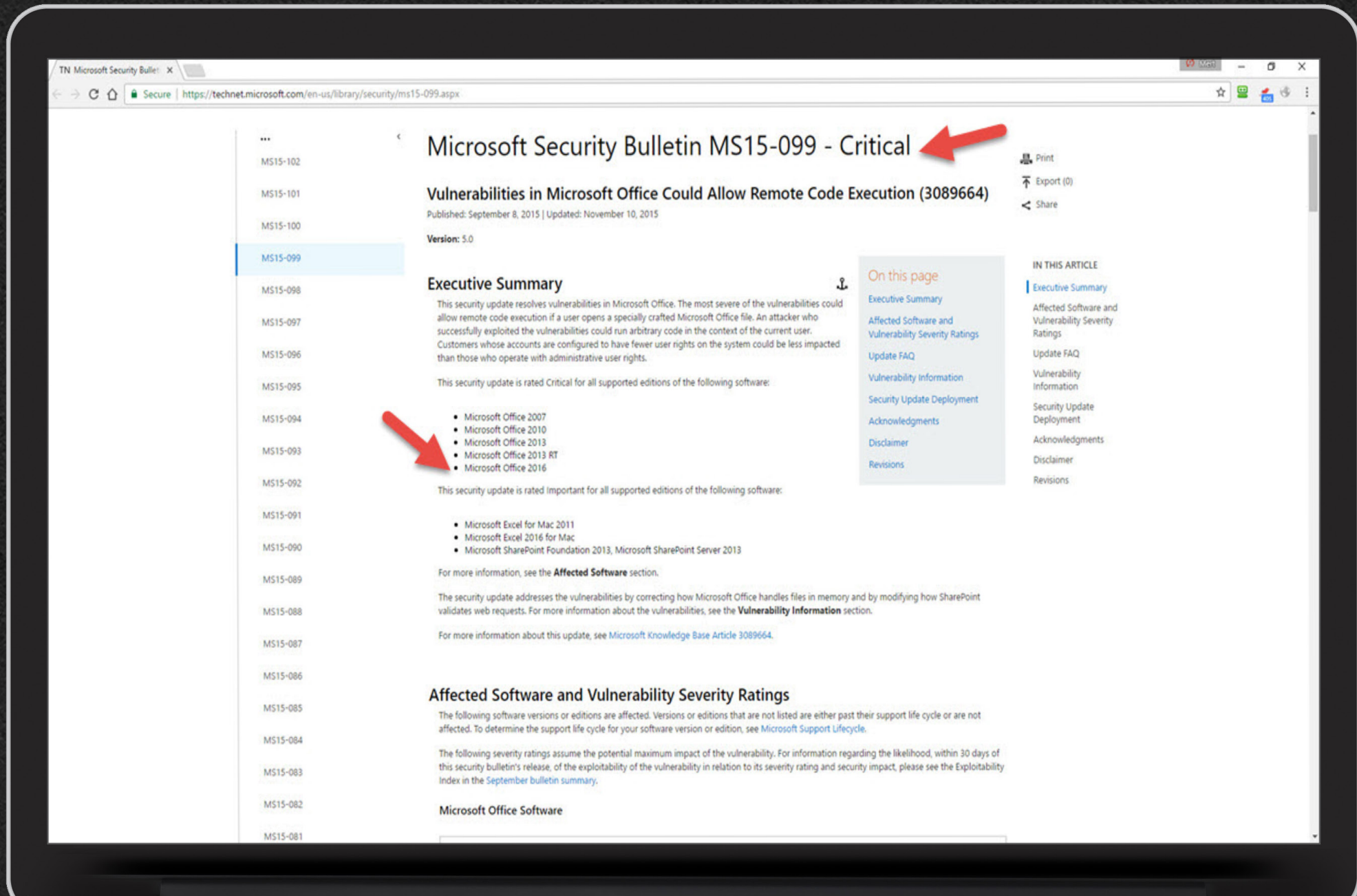


APT GİRİŞİMİ #2

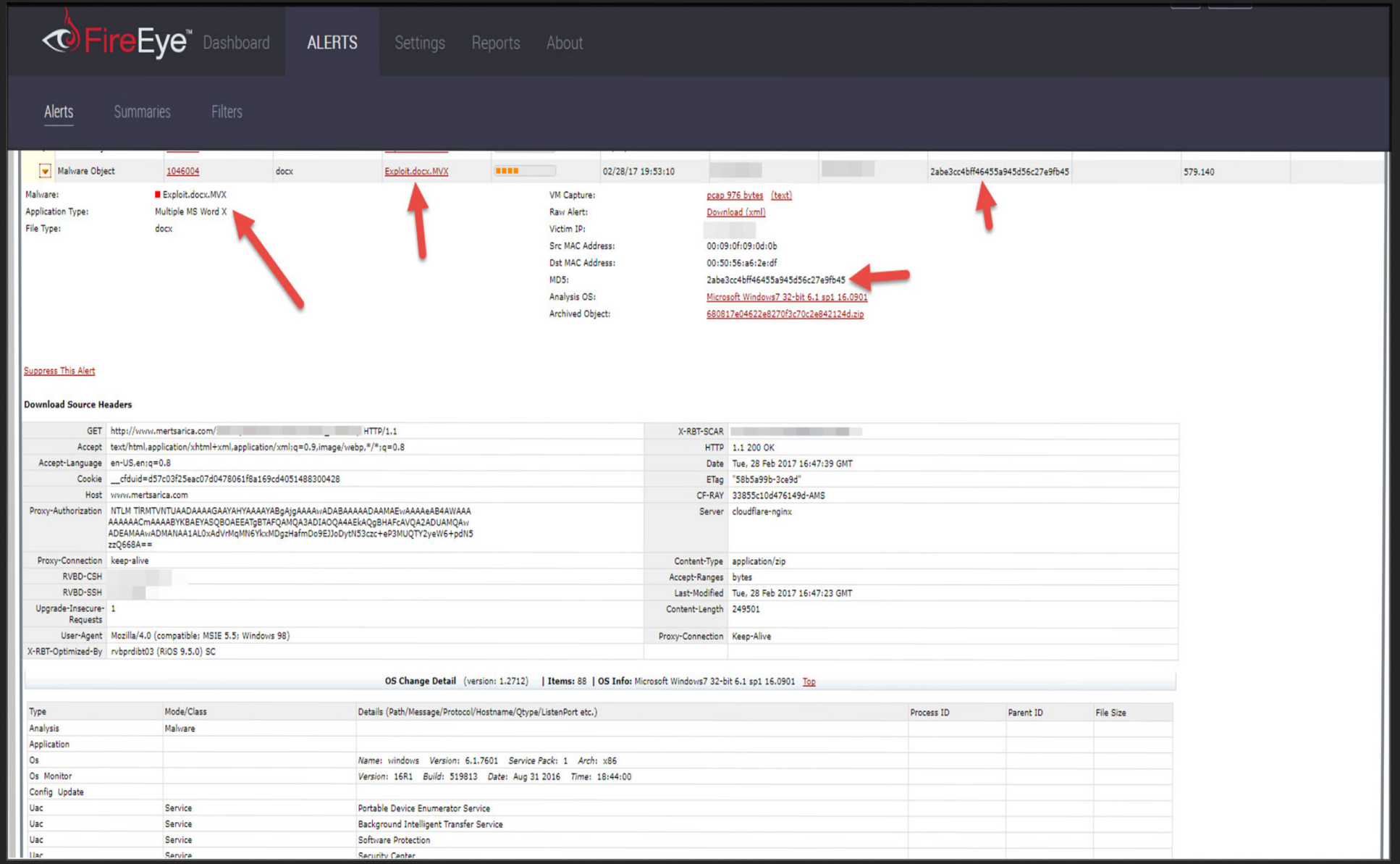


engine (58)	positiv (9)	date (dd.mm.y...	age (...
BitDefender	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Arcabit	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Ad-Aware	Exploit.CVE-2015-2545.Gen	28.02.2017	0
F-Secure	Exploit.CVE-2015-2545.Gen	28.02.2017	0
GData	Exploit.CVE-2015-2545.Gen	28.02.2017	0
Emsisoft	Exploit.CVE-2015-2545.Gen (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

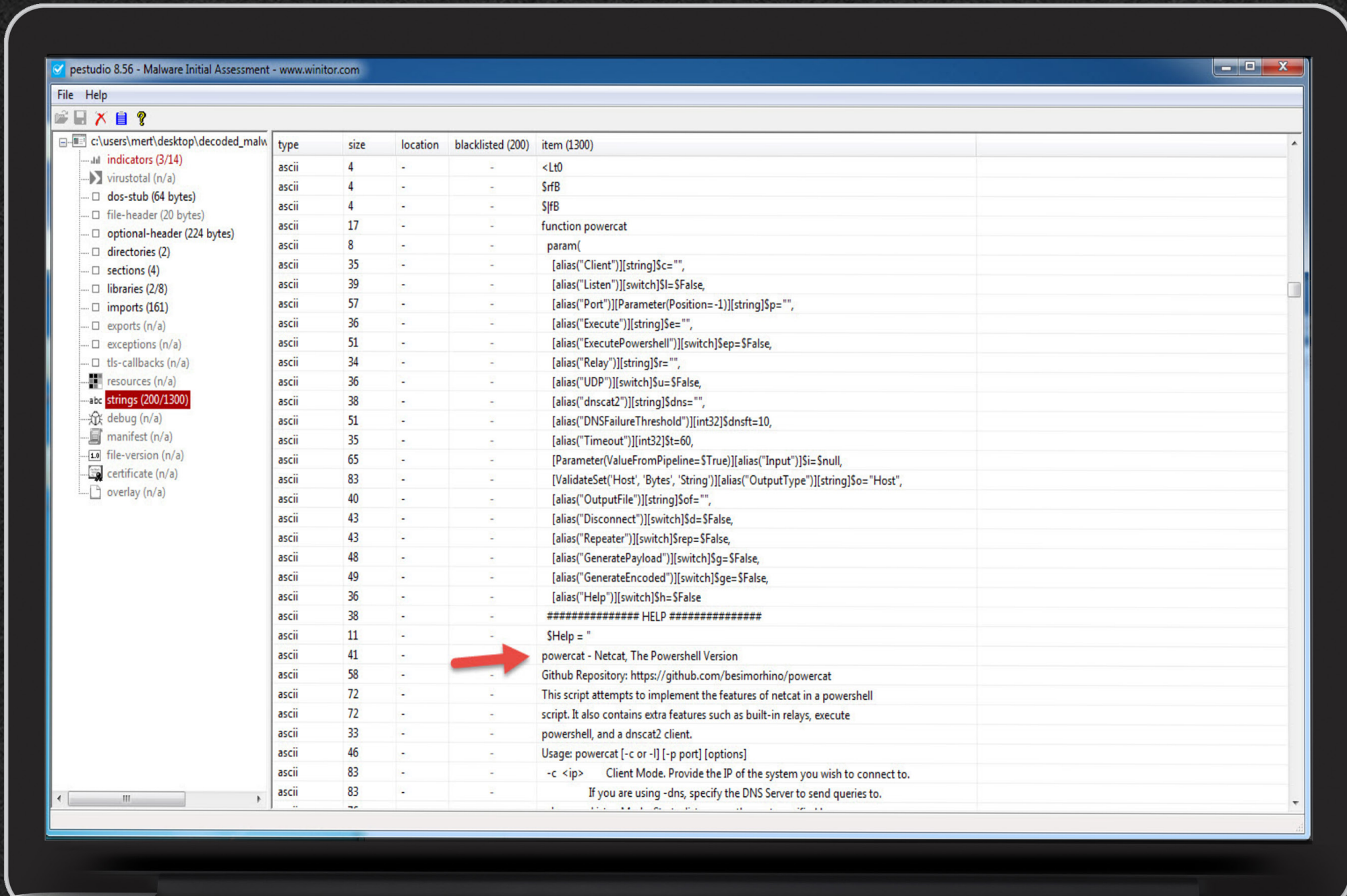
APT GİRİŞİMİ #2



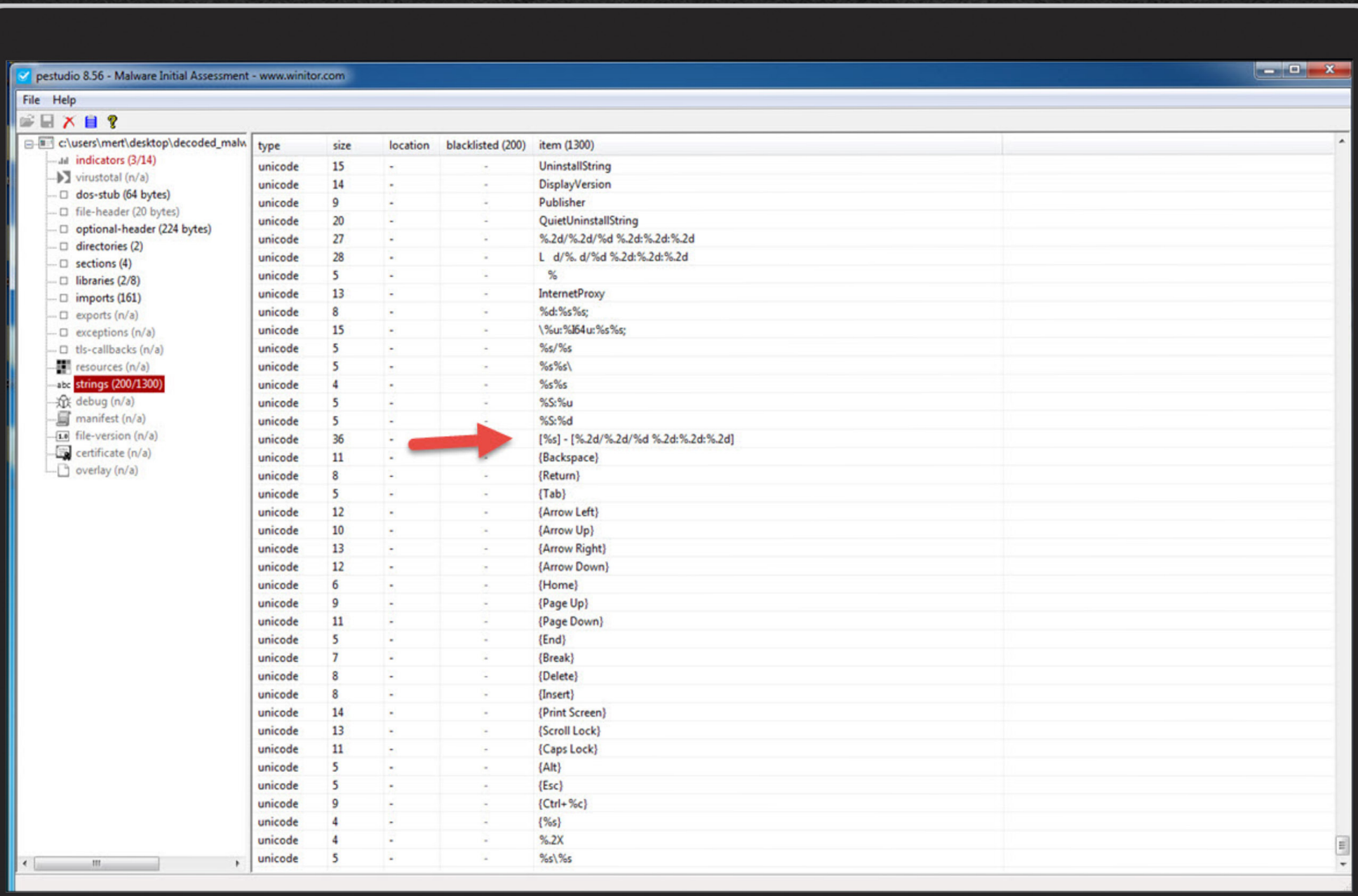
APT GİRİŞİMİ #2



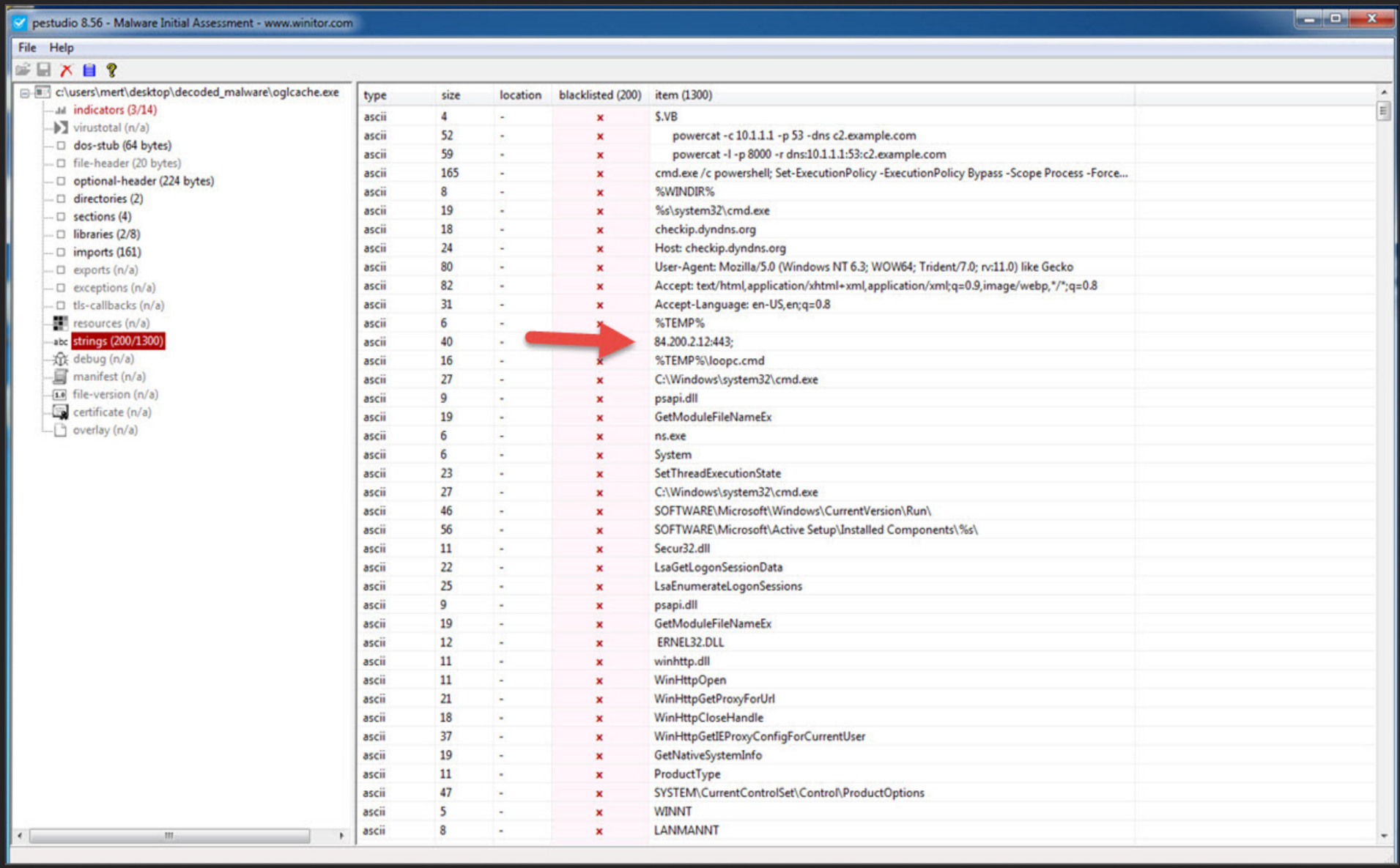
APT GİRİŞİMİ #2



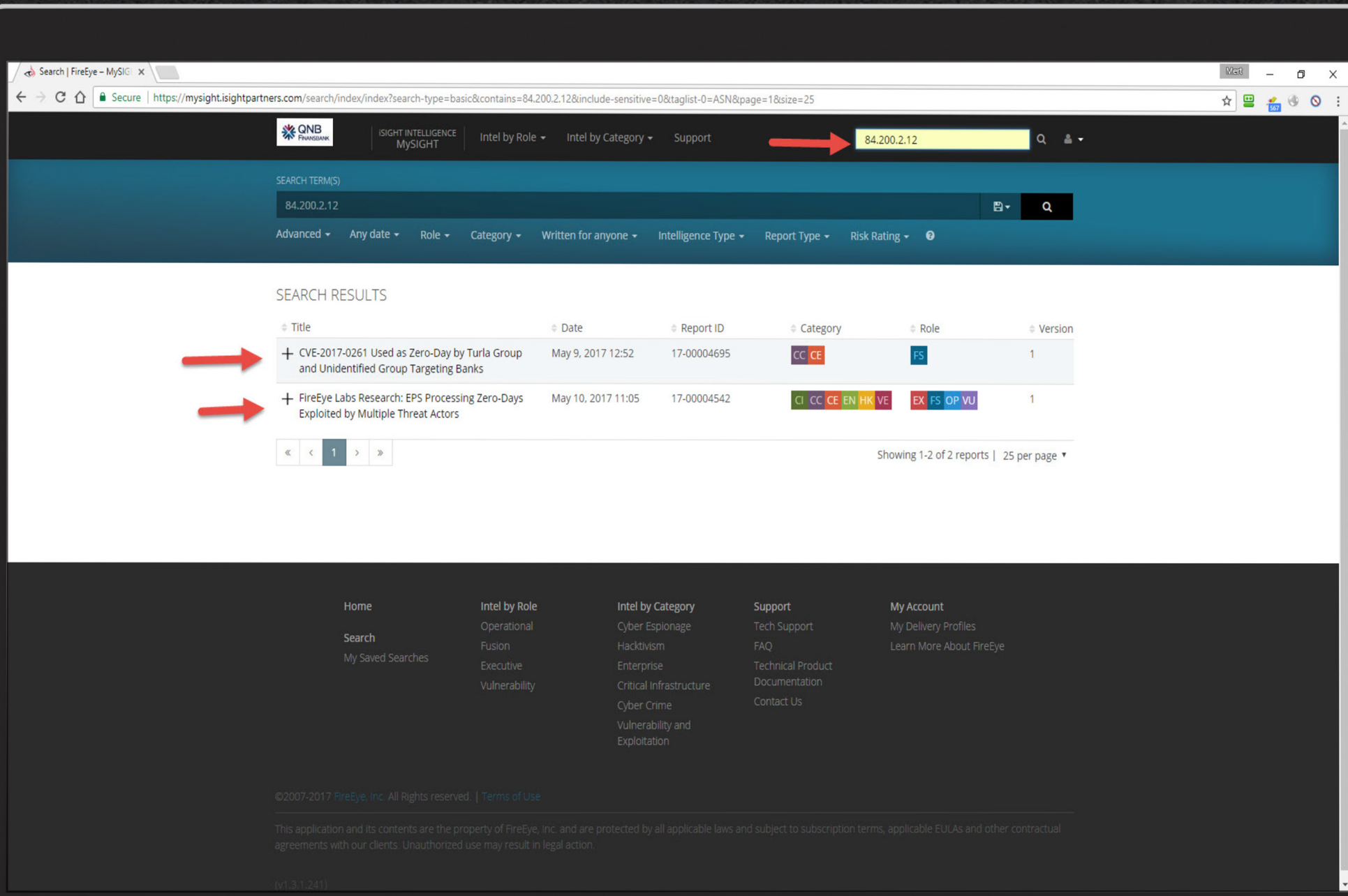
APT GİRİŞİMİ #2



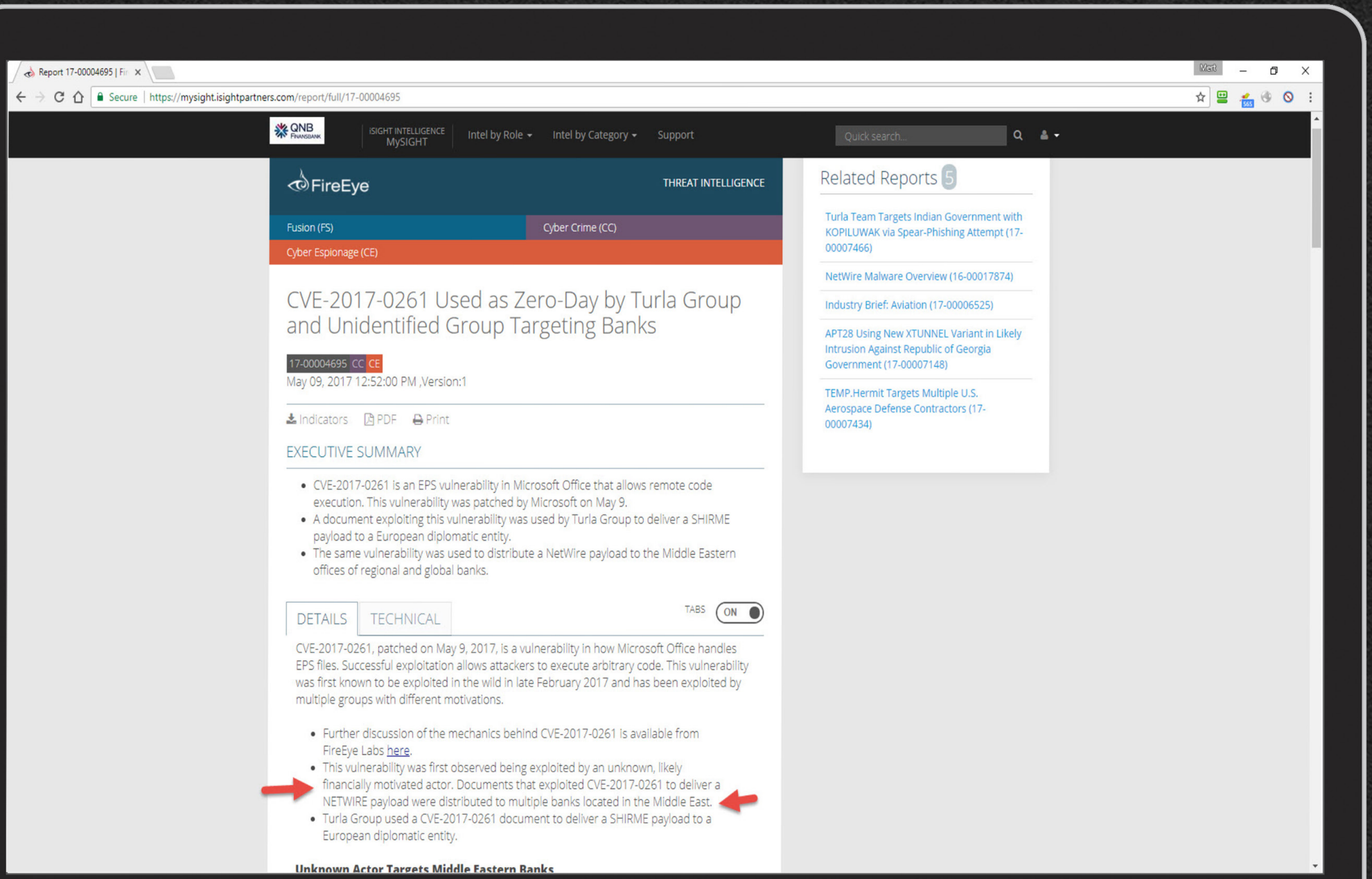
APT GİRİŞİMİ #2



APT GİRİŞİMİ #2



APT GİRİŞİMİ #2



"Zeki insanları alıp sonra onlara ne yapacaklarını söylemek mantıklı gelmiyor.
Biz zeki insanları işe alırız 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 bulundukları için FireEye firmasına teşekkür ederim. :)

SORULAR?

MUTLU SON.

 mertsarica  mertsarica

mertsarica@gmail.com

Sunum Tasarımı

MINIMALISTA

CREATIVE AGENCY

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

minimalista.com.tr minimalistacreative minimalista_creative