The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor

APT REPORTS 27 FEB 2013 2 minute read

// AUTHORS

Expert GREAT

(or, how many cool words can you fit into one title)

On Feb 12th 2013, FireEye announced the discovery of an Adobe Reader 0-day exploit which is used to drop a previously unknown, advanced piece of malware. We called this new malware ?ItaDuke because it reminded us of Duqu and because of the ancient Italian comments in the shellcode copied from Dante Alighieri-s ?Divine Comedy.

Since the original announcement, we have observed **several new attacks** using the same exploit (CVE-2013-0640) which drop other malware. Between these, we've observed a couple of incidents which are so unusual in many ways that we-ve decided to analyse them in depth.

Together with our partner CrySyS Lab, we-ve performed a detailed analysis of these unusual incidents which suggest a new, previously unknown threat actor. For the CrySyS Lab analysis, please read [here]. For our analysis, please read below.

GREAT WEBINARS

13 MAY 2021, 1:00PM
GReAT Ideas. Balalaika Edition
BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM
GReAT Ideas. Green Tea Edition
JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA, MOTOHIKO SATO

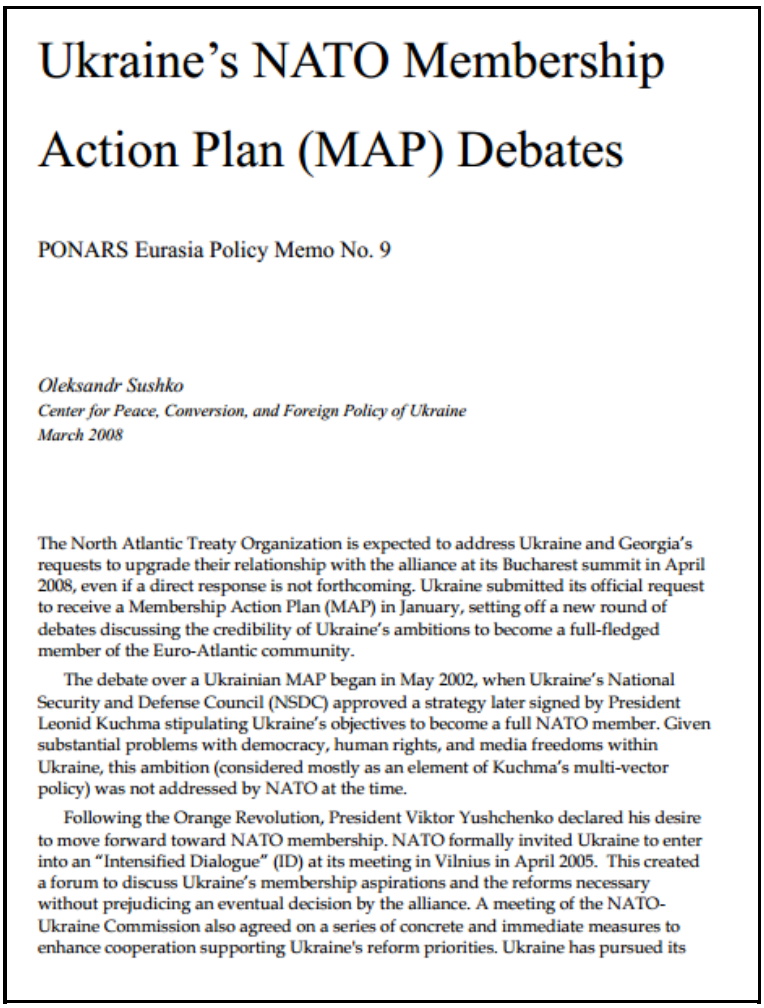
17 JUN 2020, 1:00PM
GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots
MARCO PREUSS, DENIS LEGEZO, COSTIN RAIU, KURT BAUMGARTNER, DAN DEMETER, YAROSLAV SHMELEV

26 AUG 2020, 2:00PM
GReAT Ideas. Powered by SAS: threat actors advance on new fronts
IVAN KWIATKOWSKI, MAHER YAMOUT, NOUSHIN SHABAB, PIERRE DELCHER, FÉLIX AIME, GIAMPAOLO DEDOLA, SANTIAGO PONTIROLI

22 JUL 2020, 2:00PM
GReAT Ideas. Powered by SAS: threat hunting and new techniques
DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER, BRIAN BARTHOLOMEW, BORIS LARIN, ARIEL JUNGHEIT, FABIO ASSOLINI

Key findings include:

• The MiniDuke attackers are **still active at this time** and have created malware as recently as February 20, 2013. To compromise the victims, the attackers used extremely effective social engineering techniques which involved sending malicious PDF documents to their targets. The PDFs were highly relevant and well-crafted content that fabricated human rights seminar information (ASEM) and Ukraine-s foreign policy and NATO membership plans.



Ukraine's NATO Membership Action Plan (MAP) Debates

PONARS Eurasia Policy Memo No. 9

Oleksandr Sushko
Center for Peace, Conversion, and Foreign Policy of Ukraine
March 2008

The North Atlantic Treaty Organization is expected to address Ukraine and Georgia's requests to upgrade their relationship with the alliance at its Bucharest summit in April 2008, even if a direct response is not forthcoming. Ukraine submitted its official request to receive a Membership Action Plan (MAP) in January, setting off a new round of debates discussing the credibility of Ukraine's ambitions to become a full-fledged member of the Euro-Atlantic community.

The debate over a Ukrainian MAP began in May 2002, when Ukraine's National Security and Defense Council (NSDC) approved a strategy later signed by President Leonid Kuchma stipulating Ukraine's objectives to become a full NATO member. Given substantial problems with democracy, human rights, and media freedoms within Ukraine, this ambition (considered mostly as an element of Kuchma's multi-vector policy) was not addressed by NATO at the time.

Following the Orange Revolution, President Viktor Yushchenko declared his desire to move forward toward NATO membership. NATO formally invited Ukraine to enter into an "Intensified Dialogue" (ID) at its meeting in Vilnius in April 2005. This created a forum to discuss Ukraine's membership aspirations and the reforms necessary without prejudicing an eventual decision by the alliance. A meeting of the NATO-Ukraine Commission also agreed on a series of concrete and immediate measures to enhance cooperation supporting Ukraine's reform priorities. Ukraine has pursued its

These malicious PDF files were rigged with exploits attacking Adobe Reader versions 9, 10 and 11, bypassing its sandbox.

• Once the system is exploited, a very small downloader is dropped onto the victim-s disc that-s only 20KB in size. This downloader is unique per system and contains a **customized backdoor written in Assembler**. When loaded at system boot, the downloader uses a set of mathematical calculations to determine the computer-s unique fingerprint, and in turn uses this data to uniquely

FROM THE SAME AUTHORS

APT trends report Q1 2021

APT10: sophisticated multi-layered loader Ecipekac discovered in A41APT campaign

APT annual review: What the world's threat actors got up to in 2020

Cyberthreats to financial organizations in 2021

Advanced Threat predictions for 2021

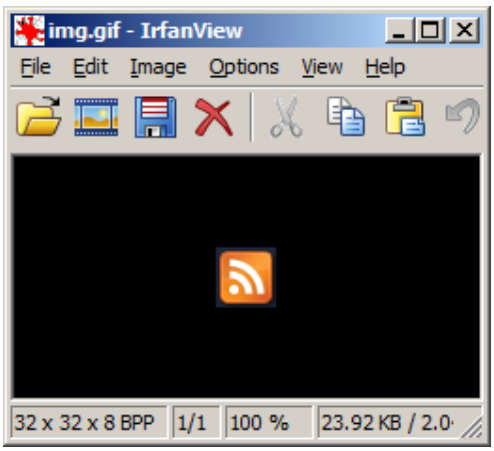
encrypt its communications later.

· If the target system meets the pre-defined requirements, the **malware will use Twitter (unbeknownst to the user) and start looking for specific tweets from pre-made accounts**. These accounts were created by MiniDuke-s Command and Control (C2) operators and the tweets maintain specific tags labeling encrypted URLs for the backdoors.

These URLs provide access to the C2s, which then provide potential commands and encrypted **transfers of additional backdoors onto the system via GIF files**.

· Based on the analysis, it appears that the MiniDuke-s creators provide a dynamic backup system that also can fly under the radar – if Twitter isn-t working or the accounts are down, **the malware can use Google Search to find the encrypted strings to the next C2**. This model is flexible and enables the operators to constantly change how their backdoors retrieve further commands or malcode as needed.

· Once the infected system locates the C2, it receives **encrypted backdoors that are obfuscated within GIF files** and disguised as pictures that appear on a victim-s machine.



Once they are downloaded to the machine, they can fetch a larger backdoor which carries out the cyberespionage activities, through functions such as copy file, move file, remove file, make directory, kill process and of course, download and execute new malware and lateral movement tools.

· The final stage backdoor **connects to two servers, one in Panama and one in Turkey** to receive the instructions from the attackers.

· The attackers **left a small clue in the code, in the form of the number 666** (0x29A hex) before one of the decryption subroutines:

```
                add     esp, 400h
                retn
CRC32           endp
; ---------------------------------------------------------------------------
                dw 666
; ---------------------------------------------------------------------------
; START OF FUNCTION CHUNK FOR DecryptURLWithSHA1
cGet128bytes:                           ; CODE XREF: DecryptURLWithSHA1+5Ij
                call    Get128bytes
; END OF FUNCTION CHUNK FOR DecryptURLWithSHA1
; ---------------------------------------------------------------------------
                dd 0
                dd 0
                dd 8834222Dh
                dd 0CFE7AE70h
```

· By analysing the logs from the command servers, we have observed **59 unique victims in 23 countries**:

Belgium, Brazil, Bulgaria, Czech Republic, Georgia, Germany, Hungary, Ireland, Israel, Japan, Latvia, Lebanon, Lithuania, Montenegro, Portugal, Romania, Russian Federation, Slovenia, Spain, Turkey, Ukraine, United Kingdom and United States.

For the detailed analysis and information on how to protect against the attack, please read:

IN THE SAME CATEGORY

BellaCPP: Discovering a new BellaCiao variant written in C++

Lazarus group evolves its infection chain with old and new malware

Careto is back: what's new after 10 years of silence?

APT trends report Q3 2024

[The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor.PDF]

APT trends report Q3 2024

Beyond the Surface: the evolution and expansion of the SideWinder APT group

ADOBE | ADOBE PDF | DATA ENCRYPTION | MINIDUKE | OBFUSCATION | TARGETED ATTACKS | VULNERABILITIES AND EXPLOITS

The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

JAGUAR3217
Posted on March 13, 2017. 6:44 pm

Is this really the number of the beast?
Is the feed logo like GIF image thing cursed?

Reply

// LATEST POSTS

SOC, TI AND IR POSTS

Attackers exploiting a patched FortiClient EMS vulnerability in the wild

ASHLEY MUÑOZ,
FRANCESCO FIGURELLI,
CRISTIAN SOUZA,
EDUARDO OVALLE,
AREG BAGHINYAN

APT REPORTS

Lazarus group evolves its infection chain with old and new malware

VASILY BERDNIKOV, SOJUN RYU

CRIMEWARE REPORTS

Analysis of Cyber Anarchy Squad attacks targeting Russian and Belarusian organizations

KASPERSKY

MALWARE DESCRIPTIONS

Download a banker to track your parcel

DMITRY KALININ

// LATEST WEBINARS

THREAT INTELLIGENCE AND IR

04 SEP 2024, 5:00PM 60 MIN

Inside the Dark Web: exploring the human side of cybercriminals

ANNA PAVLOVSKAYA

TECHNOLOGIES AND SERVICES

13 AUG 2024, 5:00PM 60 MIN

The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise

OLEG GOROBETS,
ALEXANDER LISKIN

CYBERTHREAT TALKS

16 JUL 2024, 5:00PM 60 MIN

Cybersecurity's human factor – more than an unpatched vulnerability

OLEG GOROBETS

TRAININGS AND WORKSHOPS

09 JUL 2024, 4:00PM 60 MIN

Building and prioritizing detection engineering backlogs with MITRE ATT&CK

ANDREY TAMOYKIN

// REPORTS

BellaCPP: Discovering a new BellaCiao variant written in C++

While investigating an incident involving the BellaCiao .NET malware, Kaspersky researchers discovered a C++ version they dubbed “BellaCPP”.

Lazarus group evolves its infection chain with old and new malware

Lazarus targets employees of a nuclear-related organization with a bunch of malware, such as MISTPEN, LPEClient, RollMid, CookieTime and a new modular backdoor CookiePlus.

Careto is back: what’s new after 10 years of silence?

Kaspersky researchers analyze 2019, 2022 and 2024 attacks attributed to Careto APT with medium to high confidence.

APT trends report Q3 2024

The report features the most significant developments relating to APT groups in Q3 2024, including hacktivist activity, new APT tools and campaigns.

// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

Email

Subscribe

I agree to provide my email address to “AO Kaspersky Lab” to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the “unsubscribe” link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

THREATS

APT (Targeted attacks)
Secure environment (IoT)
Mobile threats
Financial threats
Spam and phishing
Industrial threats
Web threats
Vulnerabilities and exploits
All threats

CATEGORIES

APT reports
Malware descriptions
Security Bulletin
Malware reports
Spam and phishing reports
Security technologies
Research
Publications
All categories

OTHER SECTIONS

Archive
All tags
Webinars
APT Logbook
Statistics
Encyclopedia
Threats descriptions
KSB 2024

Privacy Policy
License Agreement
Cookies