LAB REPORT

Valentine's Day Assignment

Richard Flores

Northern Virginia Community College

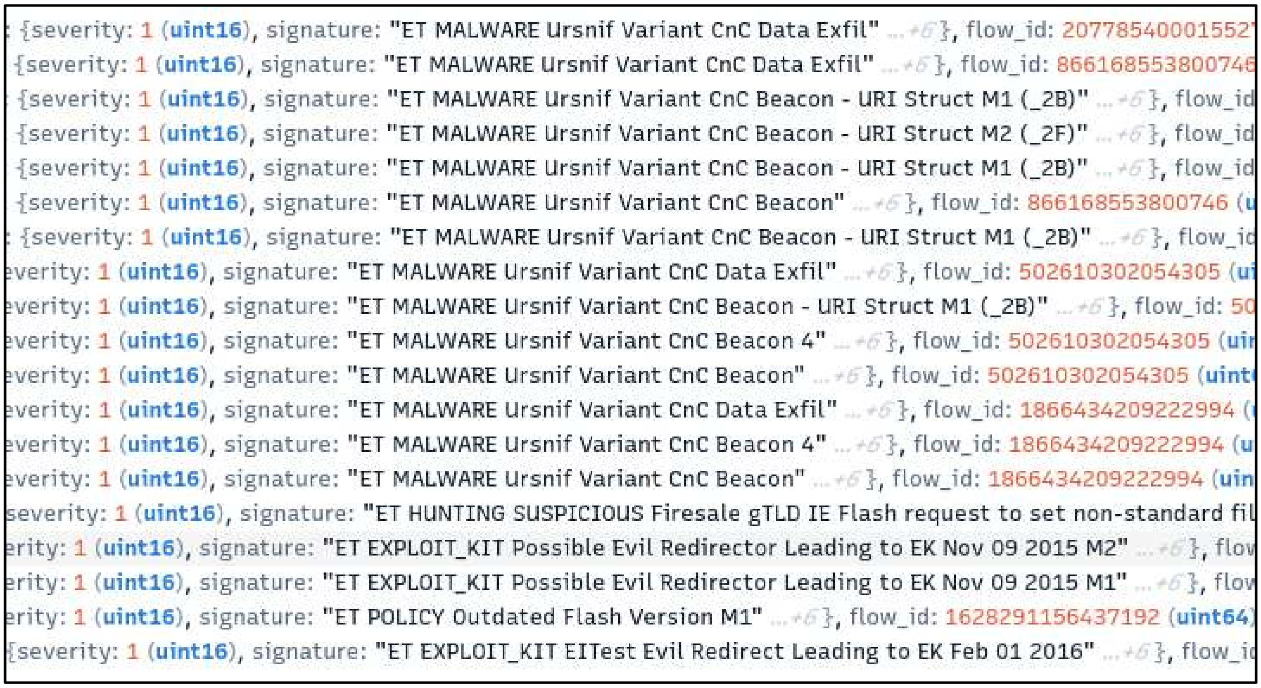
ITN 262 01YA

Prof. “Michael” Hon

December 4, 2023

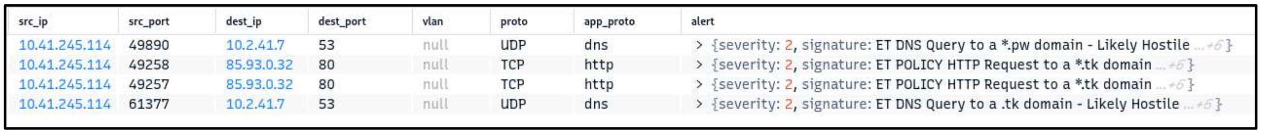
I. A summary of what happened. Be sure to include the affected employee's name and position in the company.

A. Malware was detected. Command and Control activity as well as redirection attacks.



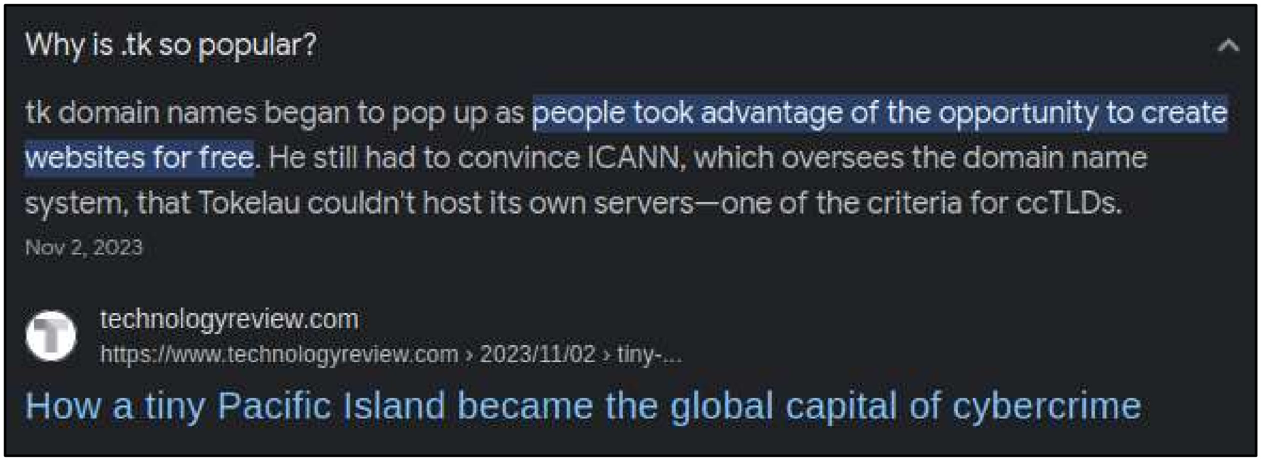
```
: {severity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Data Exfil" ... +6 }, flow_id: 20778540001552
 {severity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Data Exfil" ... +6 }, flow_id: 866168553800746
: {severity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Beacon - URI Struct M1 (_2B)" ... +6 }, flow_id
 {severity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Beacon - URI Struct M2 (_2F)" ... +6 }, flow_id
 {severity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Beacon - URI Struct M1 (_2B)" ... +6 }, flow_id
 {severity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Beacon" ... +6 }, flow_id: 866168553800746 (u
: {severity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Beacon - URI Struct M1 (_2B)" ... +6 }, flow_id
everity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Data Exfil" ... +6 }, flow_id: 502610302054305 (ui
everity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Beacon - URI Struct M1 (_2B)" ... +6 }, flow_id: 50
everity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Beacon 4" ... +6 }, flow_id: 502610302054305 (uin
everity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Beacon" ... +6 }, flow_id: 502610302054305 (uint
everity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Data Exfil" ... +6 }, flow_id: 1866434209222994 (
everity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Beacon 4" ... +6 }, flow_id: 1866434209222994 (u
everity: 1 (uint16), signature: "ET MALWARE Ursnif Variant CnC Beacon" ... +6 }, flow_id: 1866434209222994 (uin
severity: 1 (uint16), signature: "ET HUNTING SUSPICIOUS Firesale gTLD IE Flash request to set non-standard fil
erity: 1 (uint16), signature: "ET EXPLOIT_KIT Possible Evil Redirector Leading to EK Nov 09 2015 M2" ... +6 }, flow
erity: 1 (uint16), signature: "ET EXPLOIT_KIT Possible Evil Redirector Leading to EK Nov 09 2015 M1" ... +6 }, flow
erity: 1 (uint16), signature: "ET POLICY Outdated Flash Version M1" ... +6 }, flow_id: 1628291156437192 (uint64)
{severity: 1 (uint16), signature: "ET EXPLOIT_KIT EITest Evil Redirect Leading to EK Feb 01 2016" ... +6 }, flow_i
```

B. Suspicious domains were connected to flagged as likely hostile.



src_ip	src_port	dest_ip	dest_port	vlan	proto	app_proto	alert
10.41.245.114	49890	10.2.41.7	53	null	UDP	dns	> {severity: 2, signature: ET DNS Query to a *.pw domain - Likely Hostile ... +6 }
10.41.245.114	49258	85.93.0.32	80	null	TCP	http	> {severity: 2, signature: ET POLICY HTTP Request to a *.tk domain ... +6 }
10.41.245.114	49257	85.93.0.32	80	null	TCP	http	> {severity: 2, signature: ET POLICY HTTP Request to a *.tk domain ... +6 }
10.41.245.114	61377	10.2.41.7	53	null	UDP	dns	> {severity: 2, signature: ET DNS Query to a .tk domain - Likely Hostile ... +6 }

C. Google:



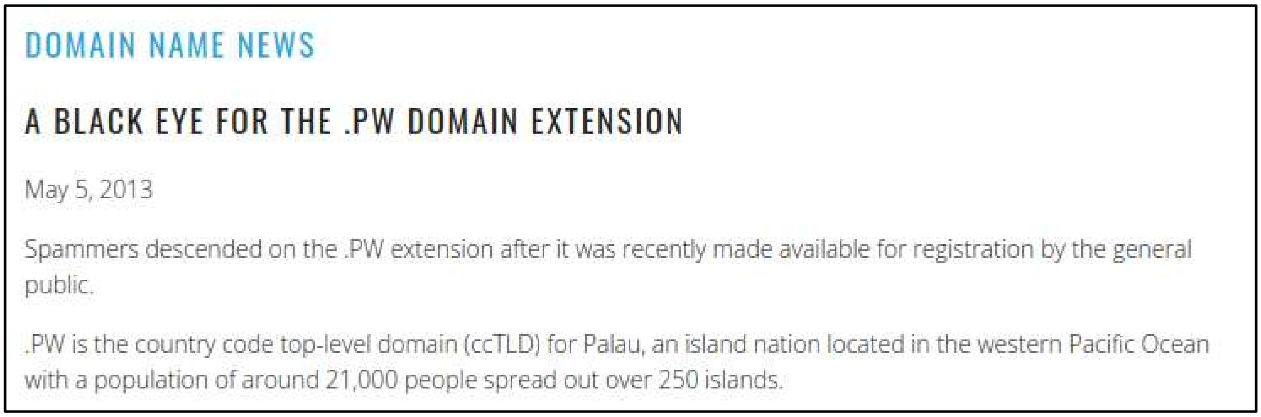
Why is .tk so popular?

tk domain names began to pop up as people took advantage of the opportunity to create websites for free. He still had to convince ICANN, which oversees the domain name system, that Tokelau couldn't host its own servers—one of the criteria for ccTLDs.

Nov 2, 2023

technologyreview.com
https://www.technologyreview.com › 2023/11/02 › tiny-...

How a tiny Pacific Island became the global capital of cybercrime



DOMAIN NAME NEWS

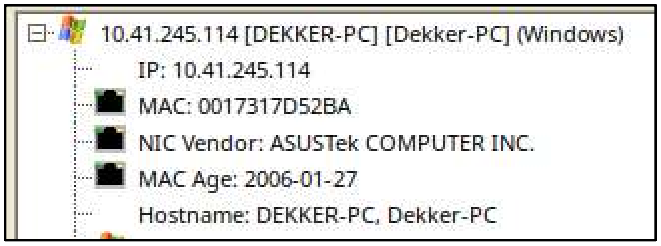
A BLACK EYE FOR THE .PW DOMAIN EXTENSION

May 5, 2013

Spammers descended on the .PW extension after it was recently made available for registration by the general public.

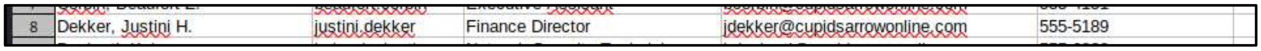
.PW is the country code top-level domain (ccTLD) for Palau, an island nation located in the western Pacific Ocean with a population of around 21,000 people spread out over 250 islands.

D. 10.41.245.114 is the Hostname Dekker-PC



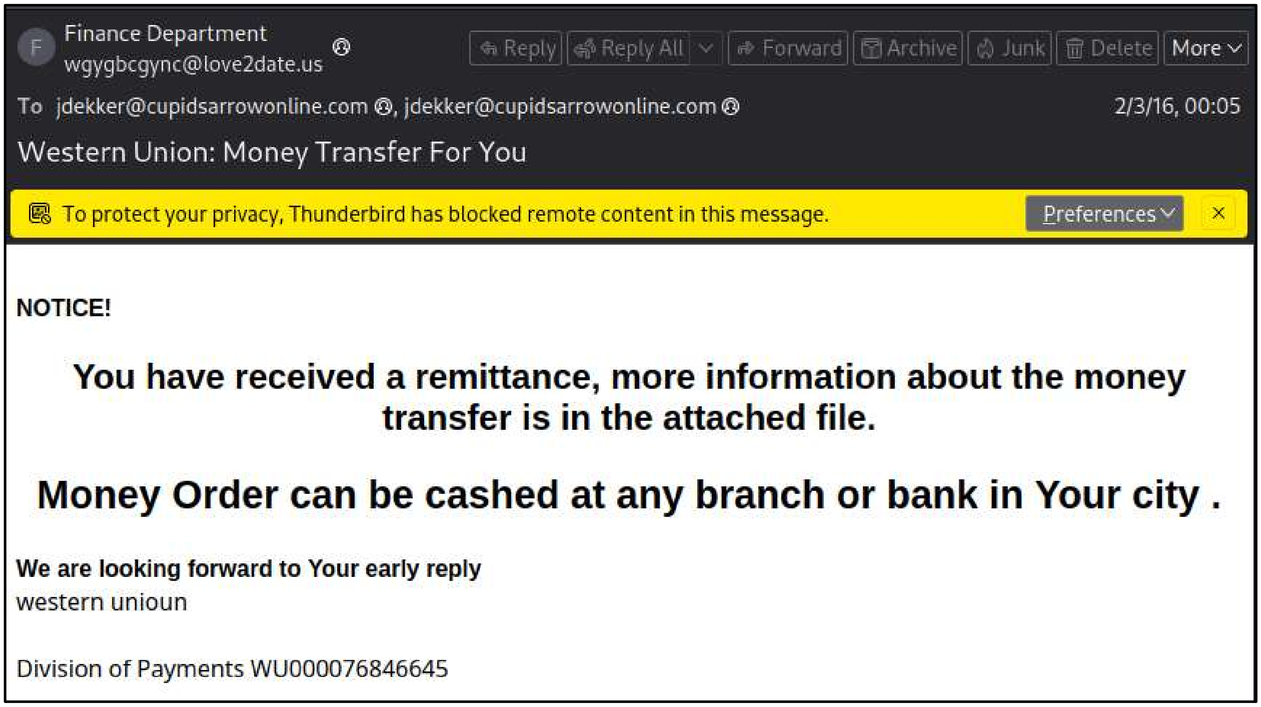
```
⊟ 10.41.245.114 [DEKKER-PC] [Dekker-PC] (Windows)
      IP: 10.41.245.114
      MAC: 0017317D52BA
      NIC Vendor: ASUSTek COMPUTER INC.
      MAC Age: 2006-01-27
      Hostname: DEKKER-PC, Dekker-PC
```

E. Employee: Justini H. Dekker, Finance Director



8	Dekker, Justini H.	justini.dekker	Finance Director	jdekker@cupidsarrowonline.com	555-5189

F. Suspicious e-mail regarding Western Union, but not from Western Union



Finance Department
wgygbcgync@love2date.us

To jdekker@cupidsarrowonline.com, jdekker@cupidsarrowonline.com 2/3/16, 00:05

Western Union: Money Transfer For You

To protect your privacy, Thunderbird has blocked remote content in this message.

NOTICE!

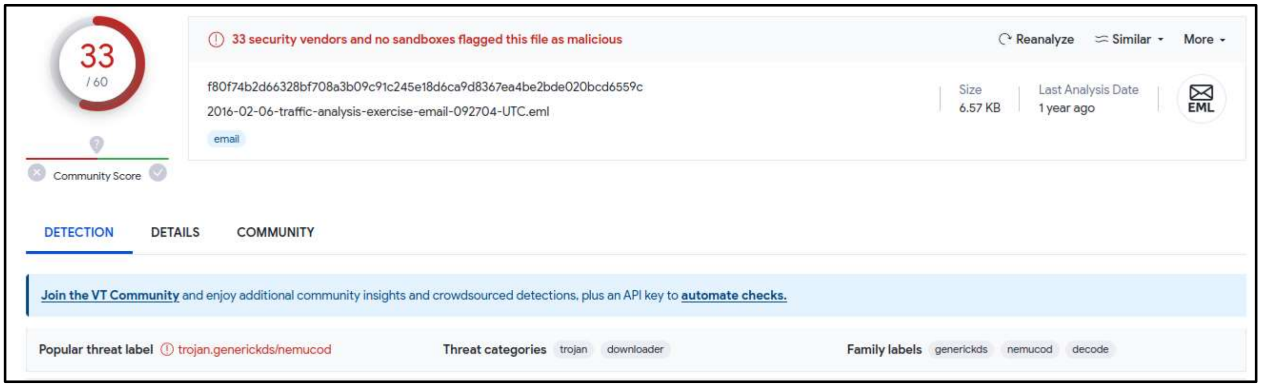
You have received a remittance, more information about the money transfer is in the attached file.

Money Order can be cashed at any branch or bank in Your city .

We are looking forward to Your early reply
western unioun

Division of Payments WU000076846645

G. This email contains a trojan: 2016-02-06-traffic-analysis-exercise-email-092704-UTC



33 security vendors and no sandboxes flagged this file as malicious

f80f74b2d66328bf708a3b09c91c245e18d6ca9d8367ea4be2bde020bcd6559c
2016-02-06-traffic-analysis-exercise-email-092704-UTC.eml
email

Size 6.57 KB

Last Analysis Date 1 year ago

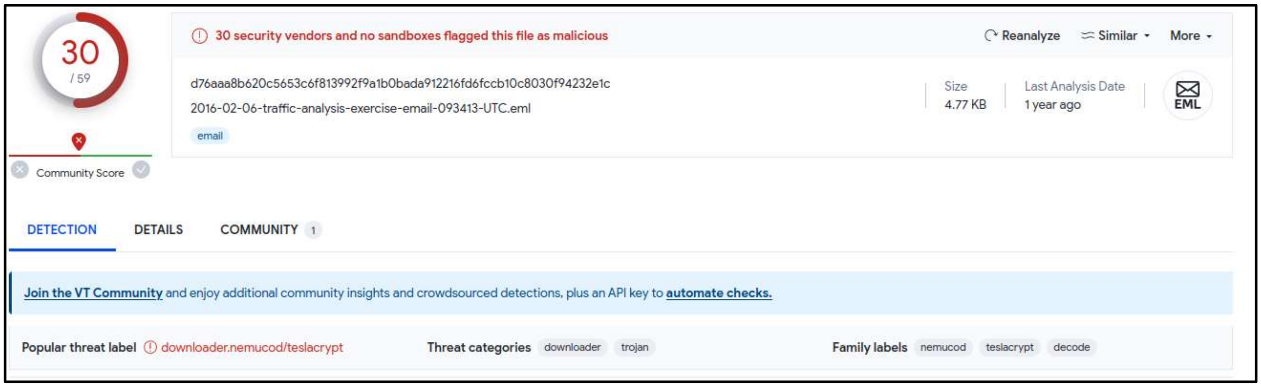
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.generickds/nemucod

Threat categories trojan downloader

Family labels generickds nemucod decode

H. This email contains cryptomalware: 2016-02-06-traffic-analysis-exercise-email-093413-UTC



30 security vendors and no sandboxes flagged this file as malicious

d76aaa8b620c5653c6f813992f9a1b0bada912216fd6fccb10c8030f94232e1c

2016-02-06-traffic-analysis-exercise-email-093413-UTC.eml

email

Size 4.77 KB

Last Analysis Date 1 year ago

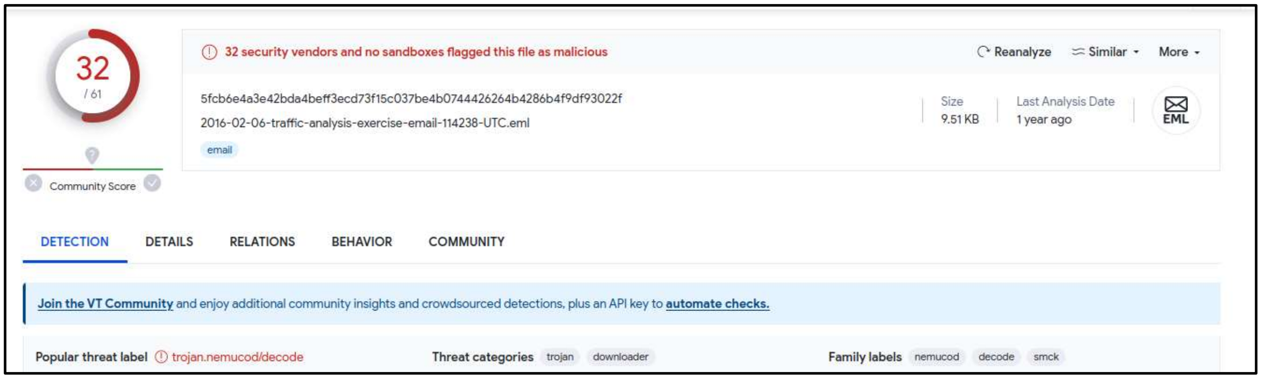
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label downloader.nemucod/teslacrypt

Threat categories downloader trojan

Family labels nemucod teslacrypt decode

I. This email contains a trojan: 2016-02-06-traffic-analysis-exercise-email-114238-UTC



32 security vendors and no sandboxes flagged this file as malicious

5fcb6e4a3e42bda4beff3ecd73f15c037be4b0744426264b4286b4f9df93022f

2016-02-06-traffic-analysis-exercise-email-114238-UTC.eml

email

Size 9.51 KB

Last Analysis Date 1 year ago

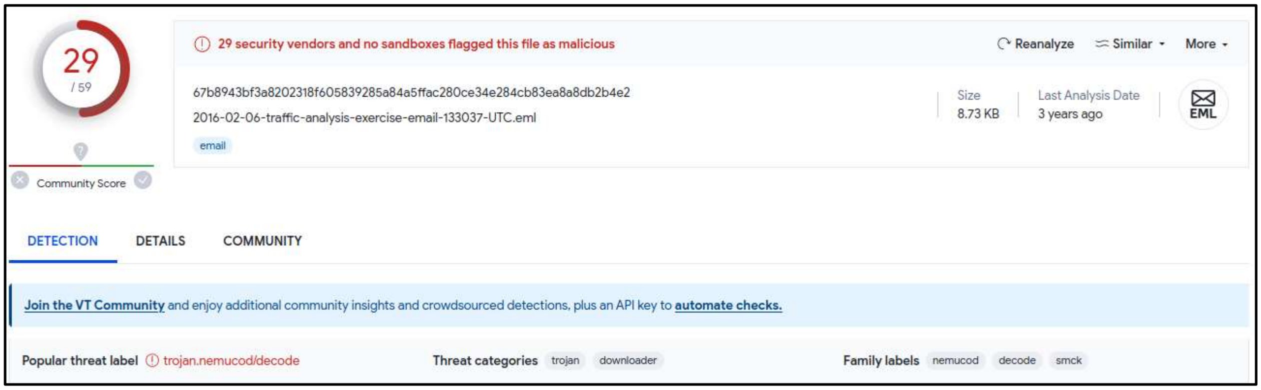
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.nemucod/decode

Threat categories trojan downloader

Family labels nemucod decode smck

J. This email contains a trojan: 2016-02-06-traffic-analysis-exercise-email-133037-UTC



29 security vendors and no sandboxes flagged this file as malicious

67b8943bf3a8202318f605839285a84a5ffac280ce34e284cb83ea8a8db2b4e2

2016-02-06-traffic-analysis-exercise-email-133037-UTC.eml

email

Size 8.73 KB

Last Analysis Date 3 years ago

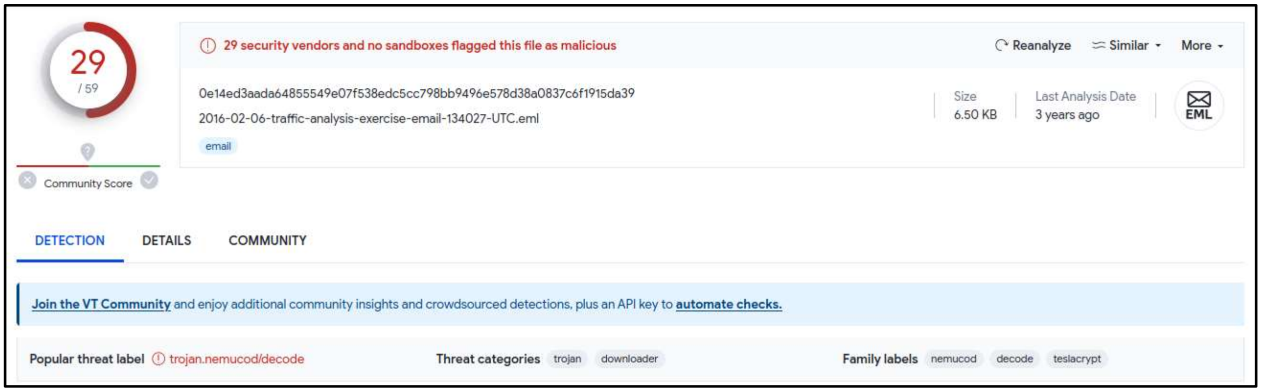
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.nemucod/decode

Threat categories trojan downloader

Family labels nemucod decode smck

K. This email contains a trojan: 2016-02-06-traffic-analysis-exercise-email-134027-UTC



29 security vendors and no sandboxes flagged this file as malicious

0e14ed3aada64855549e07f538edc5cc798bb9496e578d38a0837c6f1915da39
2016-02-06-traffic-analysis-exercise-email-134027-UTC.eml
email

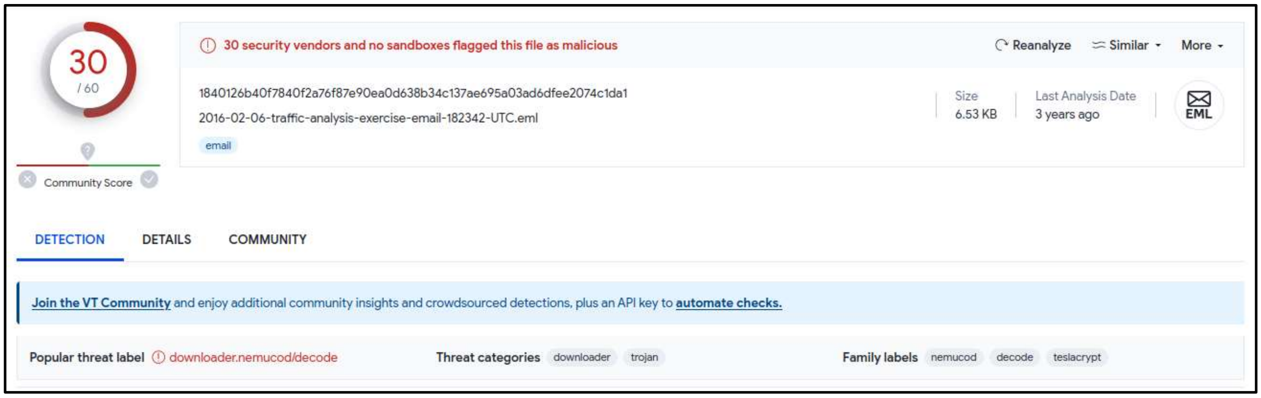
Size 6.50 KB

Last Analysis Date 3 years ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.nemucod/decode Threat categories trojan downloader Family labels nemucod decode teslacrypt

L. This email contains malware: 2016-02-06-traffic-analysis-exercise-email-182342-UTC



30 security vendors and no sandboxes flagged this file as malicious

1840126b40f7840f2a76f87e90ea0d638b34c137ae695a03ad6dfee2074c1da1
2016-02-06-traffic-analysis-exercise-email-182342-UTC.eml
email

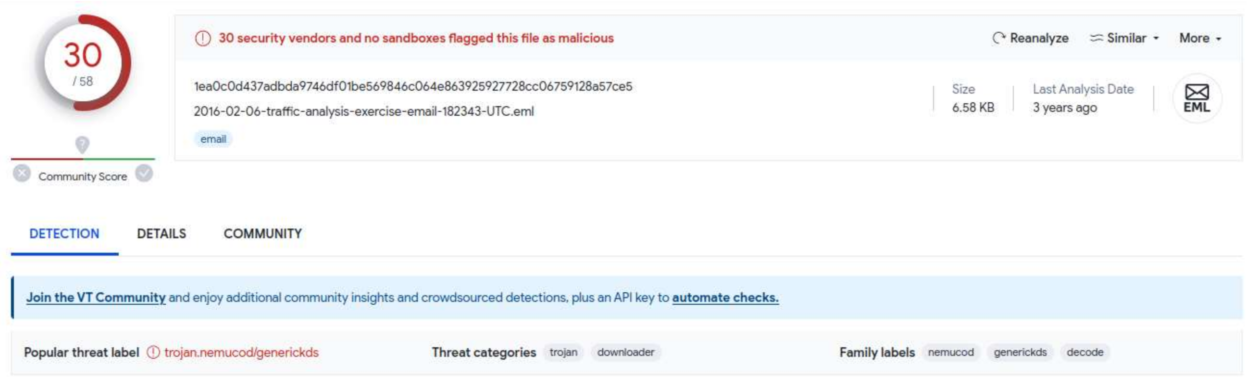
Size 6.53 KB

Last Analysis Date 3 years ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label downloader.nemucod/decode Threat categories downloader trojan Family labels nemucod decode teslacrypt

M. This email contains a trojan: 2016-02-06-traffic-analysis-exercise-email-182343-UTC



30 security vendors and no sandboxes flagged this file as malicious

1ea0c0d437adbda9746df01be569846c064e863925927728cc06759128a57ce5
2016-02-06-traffic-analysis-exercise-email-182343-UTC.eml
email

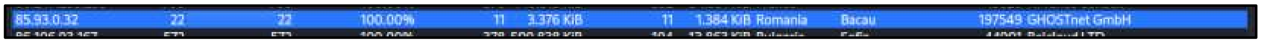
Size 6.58 KB

Last Analysis Date 3 years ago

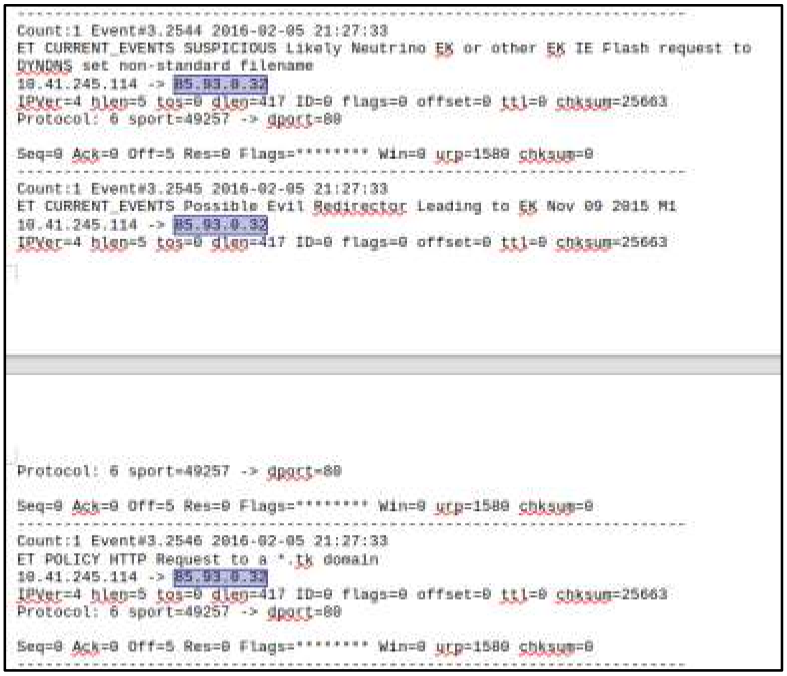
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.nemucod/generickds Threat categories trojan downloader Family labels nemucod generickds decode

N. 85.93.0.32 is either an infected site or malicious (likely malicious).



85.93.0.32	22	22	100.00%	11	3.376 KiB	11	1.384 KiB	Romania	Bacau	197549 GHOSTnet GmbH



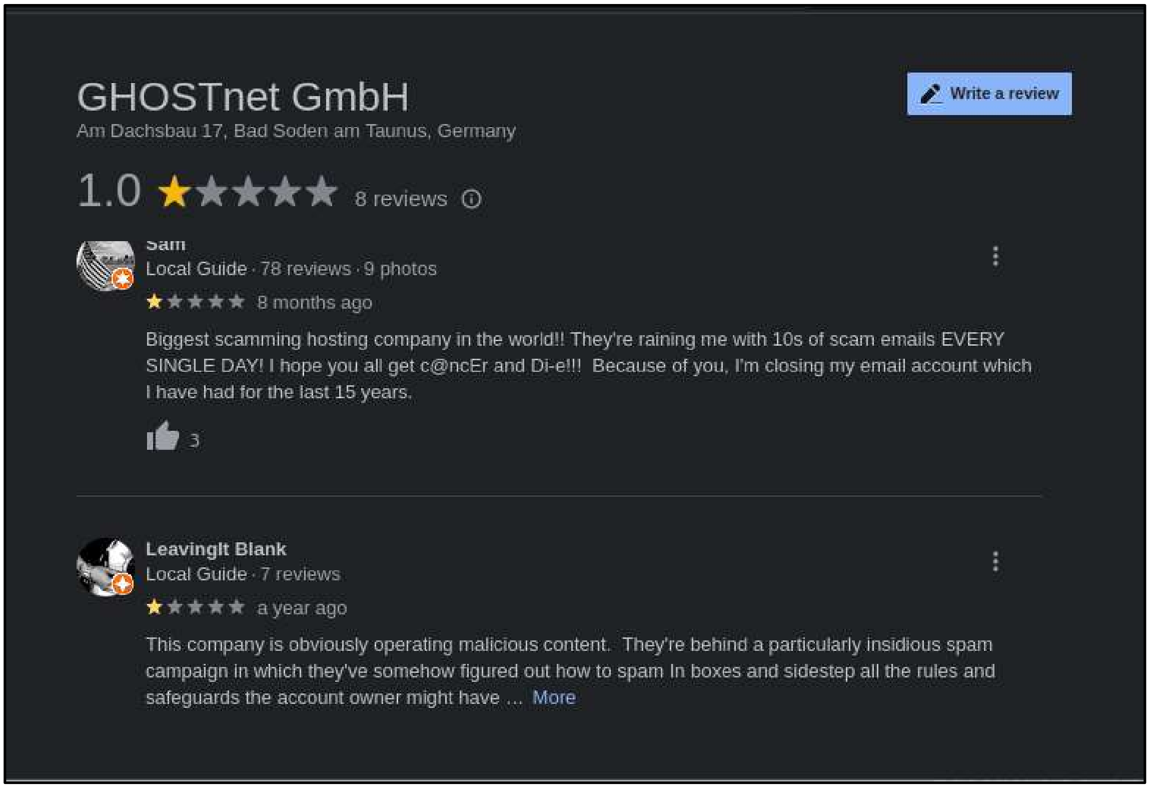
```
------------------------------------------------------------------------------
Count:1 Event#3.2544 2016-02-05 21:27:33
ET CURRENT_EVENTS SUSPICIOUS Likely Neutrino EK or other EK IE Flash request to
DYNDNS set non-standard filename
10.41.245.114 -> 85.93.0.32
IPVer=4 hlen=5 tos=0 dlen=417 ID=0 flags=0 offset=0 ttl=0 chksum=25663
Protocol: 6 sport=49257 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=1580 chksum=0
------------------------------------------------------------------------------
Count:1 Event#3.2545 2016-02-05 21:27:33
ET CURRENT_EVENTS Possible Evil Redirector Leading to EK Nov 09 2015 M1
10.41.245.114 -> 85.93.0.32
IPVer=4 hlen=5 tos=0 dlen=417 ID=0 flags=0 offset=0 ttl=0 chksum=25663

Protocol: 6 sport=49257 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=1580 chksum=0
------------------------------------------------------------------------------
Count:1 Event#3.2546 2016-02-05 21:27:33
ET POLICY HTTP Request to a *.tk domain
10.41.245.114 -> 85.93.0.32
IPVer=4 hlen=5 tos=0 dlen=417 ID=0 flags=0 offset=0 ttl=0 chksum=25663
Protocol: 6 sport=49257 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=1580 chksum=0
------------------------------------------------------------------------------
```



GHOSTnet GmbH

Am Dachsbau 17, Bad Soden am Taunus, Germany

1.0 ★★★★★ 8 reviews ⓘ

Sam

Local Guide · 78 reviews · 9 photos

★★★★★ 8 months ago

Biggest scamming hosting company in the world!! They're raining me with 10s of scam emails EVERY SINGLE DAY! I hope you all get c@ncEr and Di-e!!! Because of you, I'm closing my email account which I have had for the last 15 years.

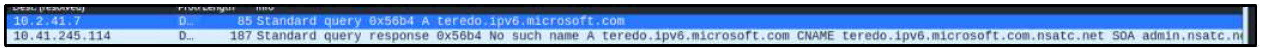
LeavingIt Blank

Local Guide · 7 reviews

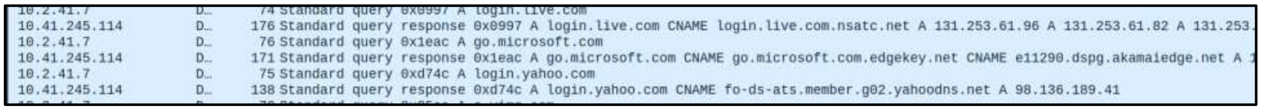
★★★★★ a year ago

This company is obviously operating malicious content. They're behind a particularly insidious spam campaign in which they've somehow figured out how to spam In boxes and sidestep all the rules and safeguards the account owner might have … More

O. 41.2.41.7 is likely malicious. Trying to hide the actual domains by using deceptive subdomains. Multiple suspicious domains.



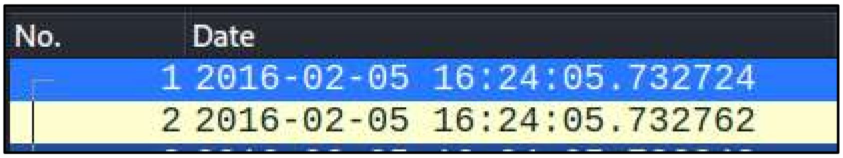
```
10.2.41.7           D…     85 Standard query 0x56b4 A teredo.ipv6.microsoft.com
10.41.245.114       D…    187 Standard query response 0x56b4 No such name A teredo.ipv6.microsoft.com CNAME teredo.ipv6.microsoft.com.nsatc.net SOA admin.nsatc.n
```



```
10.2.41.7           D…     74 Standard query 0x0997 A login.live.com
10.41.245.114       D…    176 Standard query response 0x0997 A login.live.com CNAME login.live.com.nsatc.net A 131.253.61.96 A 131.253.61.82 A 131.253.
10.2.41.7           D…     76 Standard query 0x1eac A go.microsoft.com
10.41.245.114       D…    171 Standard query response 0x1eac A go.microsoft.com CNAME go.microsoft.com.edgekey.net CNAME e11290.dspg.akamaiedge.net A 1
10.2.41.7           D…     75 Standard query 0xd74c A login.yahoo.com
10.41.245.114       D…    138 Standard query response 0xd74c A login.yahoo.com CNAME fo-ds-ats.member.g02.yahoodns.net A 98.136.189.41
```

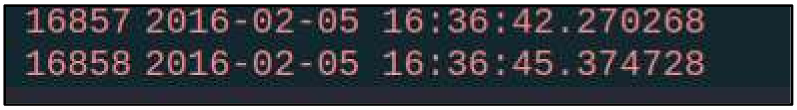
II. Date and time of the activity.

A. February 5, 2016 from 16:24 to 16:36



```
No.        Date
         1 2016-02-05 16:24:05.732724
         2 2016-02-05 16:24:05.732762
```

…



```
16857 2016-02-05 16:36:42.270268
16858 2016-02-05 16:36:45.374728
```

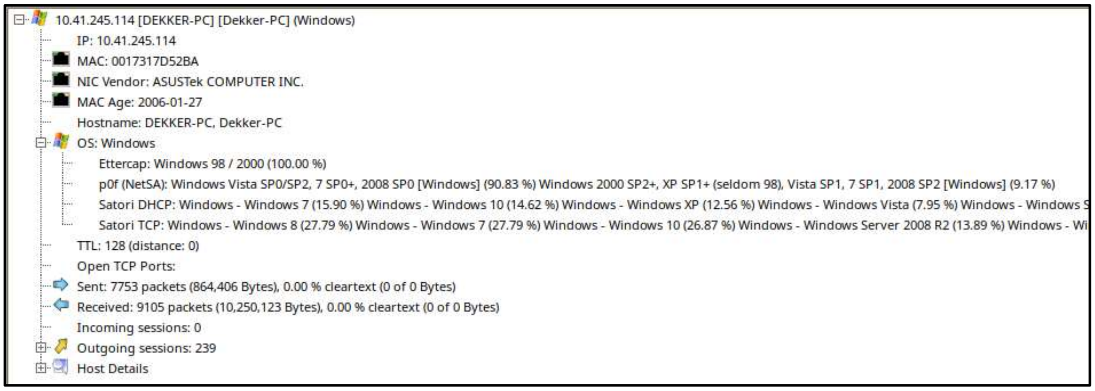
III. IP address, MAC address, and host name of the computer that was involved.

A. Victim: Dekker-PC

IP: 10.41.245.114

MAC: 0017317D52BA

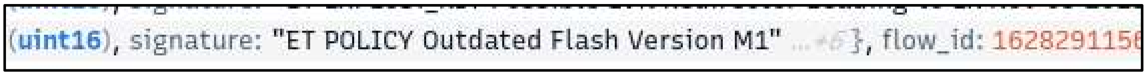
Hostname: Dekker-PC



```
10.41.245.114 [DEKKER-PC] [Dekker-PC] (Windows)
    IP: 10.41.245.114
    MAC: 0017317D52BA
    NIC Vendor: ASUSTek COMPUTER INC.
    MAC Age: 2006-01-27
    Hostname: DEKKER-PC, Dekker-PC
    OS: Windows
        Ettercap: Windows 98 / 2000 (100.00 %)
        p0f (NetSA): Windows Vista SP0/SP2, 7 SP0+, 2008 SP0 [Windows] (90.83 %) Windows 2000 SP2+, XP SP1+ (seldom 98), Vista SP1, 7 SP1, 2008 SP2 [Windows] (9.17 %)
        Satori DHCP: Windows - Windows 7 (15.90 %) Windows - Windows 10 (14.62 %) Windows - Windows XP (12.56 %) Windows - Windows Vista (7.95 %) Windows - Windows S
        Satori TCP: Windows - Windows 8 (27.79 %) Windows - Windows 7 (27.79 %) Windows - Windows 10 (26.87 %) Windows - Windows Server 2008 R2 (13.89 %) Windows - Wi
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 7753 packets (864,406 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 9105 packets (10,250,123 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 239
    Host Details
```

IV. A conclusion with recommendations for any follow-up actions, if required.

A. FLASH is vulnerable. Uninstall.



```
(uint16), signature: "ET POLICY Outdated Flash Version M1" ... +6 }, flow_id: 1628291156
```

B. Implement mandatory IT training for employees, including paying attention to links that have sneaky domains/subdomains that are trying to misdirect people.

C. Implement an email filter that blocks suspicious emails from known bad addresses, or that are flagged by anti-virus/malware, Suricata, or Snort alerts so that the emails are never even delivered.