#RSAC

RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: **SPO3-T08**

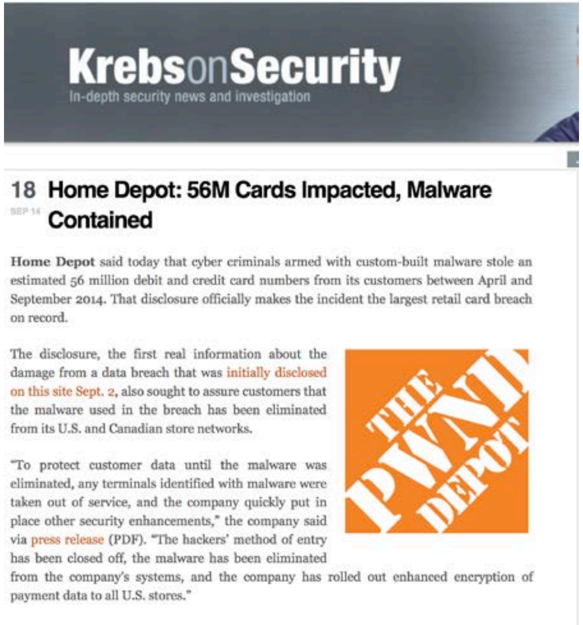
THREAT INTELLIGENCE INSIGHTS— DNS-BASED DATA EXFILTRATION IN THE WILD

Asaf Nadler

Senior Security Researcher
Akamai Technologies Inc.
@AsafNadler on Twitter

Data Exfiltration over the DNS

2014 – FrameworkPOS Malware



KrebsonSecurity
In-depth security news and investigation

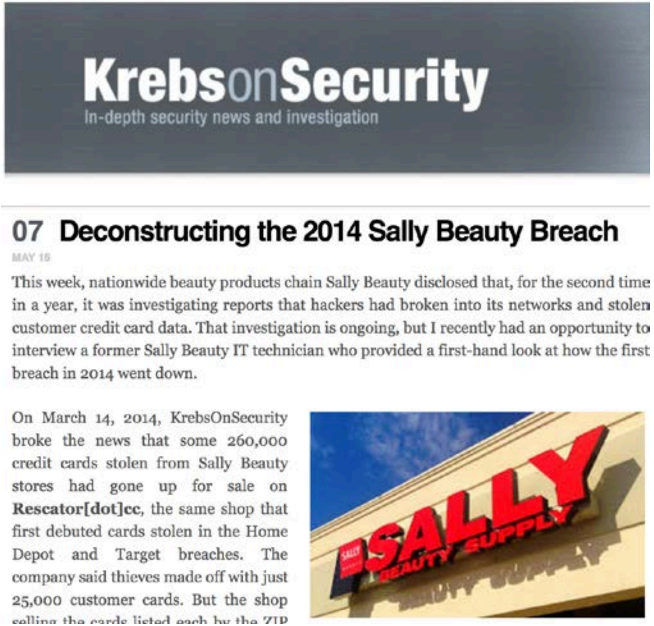
18 SEP 14 **Home Depot: 56M Cards Impacted, Malware Contained**

Home Depot said today that cyber criminals armed with custom-built malware stole an estimated 56 million debit and credit card numbers from its customers between April and September 2014. That disclosure officially makes the incident the largest retail card breach on record.

The disclosure, the first real information about the damage from a data breach that was initially disclosed on this site Sept. 2, also sought to assure customers that the malware used in the breach has been eliminated from its U.S. and Canadian store networks.

"To protect customer data until the malware was eliminated, any terminals identified with malware were taken out of service, and the company quickly put in place other security enhancements," the company said via press release (PDF). "The hackers' method of entry has been closed off, the malware has been eliminated from the company's systems, and the company has rolled out enhanced encryption of payment data to all U.S. stores."

2014 – Sally Beauty Breach



KrebsonSecurity
In-depth security news and investigation

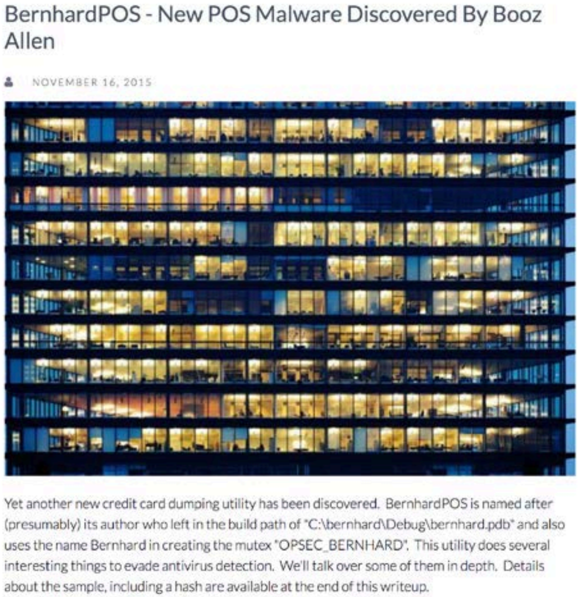
07 MAY 15 **Deconstructing the 2014 Sally Beauty Breach**

This week, nationwide beauty products chain Sally Beauty disclosed that, for the second time in a year, it was investigating reports that hackers had broken into its networks and stolen customer credit card data. That investigation is ongoing, but I recently had an opportunity to interview a former Sally Beauty IT technician who provided a first-hand look at how the first breach in 2014 went down.

On March 14, 2014, KrebsOnSecurity broke the news that some 260,000 credit cards stolen from Sally Beauty stores had gone up for sale on **Rescator[dot]cc**, the same shop that first debuted cards stolen in the Home Depot and Target breaches. The company said thieves made off with just 25,000 customer cards. But the shop selling the cards listed each by the ZIP

Data Exfiltration over the DNS

2015 – BernhardPOS Malware

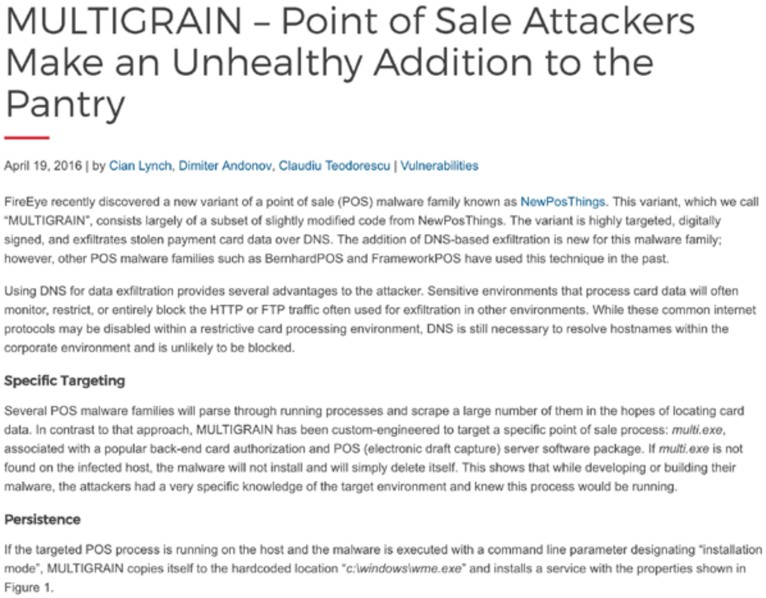


BernhardPOS - New POS Malware Discovered By Booz Allen

NOVEMBER 16, 2015

Yet another new credit card dumping utility has been discovered. BernhardPOS is named after (presumably) its author who left in the build path of "C:\bernhard\Debug\bernhard.pdb" and also uses the name Bernhard in creating the mutex "OPSEC_BERNHARD". This utility does several interesting things to evade antivirus detection. We'll talk over some of them in depth. Details about the sample, including a hash are available at the end of this writeup.

2016 – MULTIGRAIN Malware



MULTIGRAIN – Point of Sale Attackers Make an Unhealthy Addition to the Pantry

April 19, 2016 | by Cian Lynch, Dimiter Andonov, Claudiu Teodorescu | Vulnerabilities

FireEye recently discovered a new variant of a point of sale (POS) malware family known as NewPosThings. This variant, which we call "MULTIGRAIN", consists largely of a subset of slightly modified code from NewPosThings. The variant is highly targeted, digitally signed, and exfiltrates stolen payment card data over DNS. The addition of DNS-based exfiltration is new for this malware family; however, other POS malware families such as BernhardPOS and FrameworkPOS have used this technique in the past.

Using DNS for data exfiltration provides several advantages to the attacker. Sensitive environments that process card data will often monitor, restrict, or entirely block the HTTP or FTP traffic often used for exfiltration in other environments. While these common internet protocols may be disabled within a restrictive card processing environment, DNS is still necessary to resolve hostnames within the corporate environment and is unlikely to be blocked.

Specific Targeting

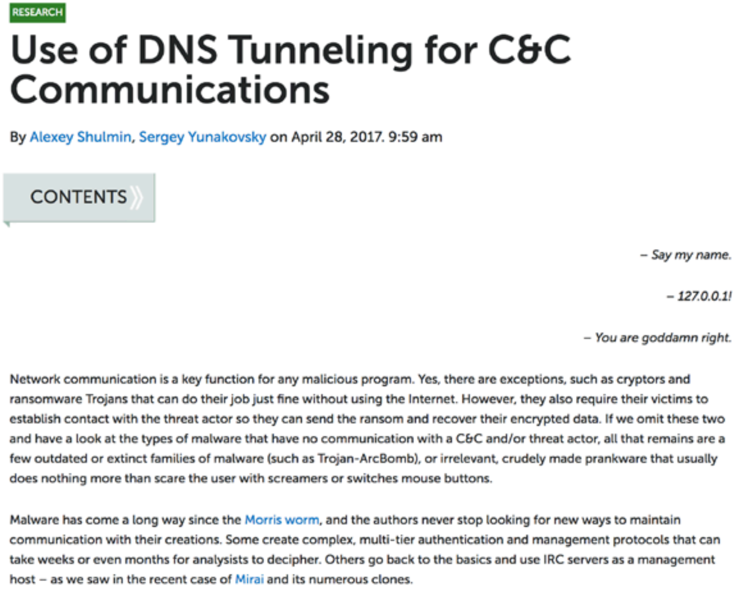
Several POS malware families will parse through running processes and scrape a large number of them in the hopes of locating card data. In contrast to that approach, MULTIGRAIN has been custom-engineered to target a specific point of sale process: *multi.exe*, associated with a popular back-end card authorization and POS (electronic draft capture) server software package. If *multi.exe* is not found on the infected host, the malware will not install and will simply delete itself. This shows that while developing or building their malware, the attackers had a very specific knowledge of the target environment and knew this process would be running.

Persistence

If the targeted POS process is running on the host and the malware is executed with a command line parameter designating "installation mode", MULTIGRAIN copies itself to the hardcoded location "*c:\windows\wme.exe*" and installs a service with the properties shown in Figure 1.

Data Exfiltration over the DNS

2017 – Win32.Backdoor.Denis



RESEARCH

Use of DNS Tunneling for C&C Communications

By Alexey Shulmin, Sergey Yunakovsky on April 28, 2017. 9:59 am

CONTENTS

– Say my name.

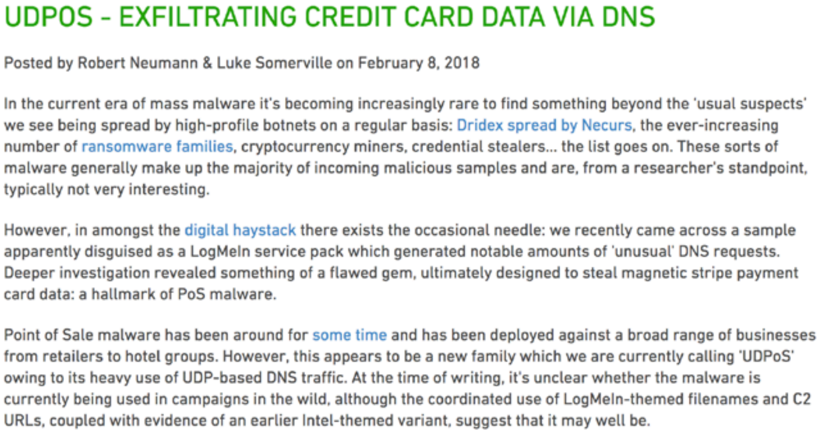
– 127.0.0.1!

– You are goddamn right.

Network communication is a key function for any malicious program. Yes, there are exceptions, such as cryptors and ransomware Trojans that can do their job just fine without using the Internet. However, they also require their victims to establish contact with the threat actor so they can send the ransom and recover their encrypted data. If we omit these two and have a look at the types of malware that have no communication with a C&C and/or threat actor, all that remains are a few outdated or extinct families of malware (such as Trojan-ArcBomb), or irrelevant, crudely made prankware that usually does nothing more than scare the user with screamers or switches mouse buttons.

Malware has come a long way since the Morris worm, and the authors never stop looking for new ways to maintain communication with their creations. Some create complex, multi-tier authentication and management protocols that can take weeks or even months for analysists to decipher. Others go back to the basics and use IRC servers as a management host – as we saw in the recent case of Mirai and its numerous clones.

2018 – UDPoS Malware



UDPOS - EXFILTRATING CREDIT CARD DATA VIA DNS

Posted by Robert Neumann & Luke Somerville on February 8, 2018

In the current era of mass malware it's becoming increasingly rare to find something beyond the 'usual suspects' we see being spread by high-profile botnets on a regular basis: Dridex spread by Necurs, the ever-increasing number of ransomware families, cryptocurrency miners, credential stealers... the list goes on. These sorts of malware generally make up the majority of incoming malicious samples and are, from a researcher's standpoint, typically not very interesting.

However, in amongst the digital haystack there exists the occasional needle: we recently came across a sample apparently disguised as a LogMeIn service pack which generated notable amounts of 'unusual' DNS requests. Deeper investigation revealed something of a flawed gem, ultimately designed to steal magnetic stripe payment card data: a hallmark of PoS malware.

Point of Sale malware has been around for some time and has been deployed against a broad range of businesses from retailers to hotel groups. However, this appears to be a new family which we are currently calling 'UDPoS' owing to its heavy use of UDP-based DNS traffic. At the time of writing, it's unclear whether the malware is currently being used in campaigns in the wild, although the coordinated use of LogMeIn-themed filenames and C2 URLs, coupled with evidence of an earlier Intel-themed variant, suggest that it may well be.

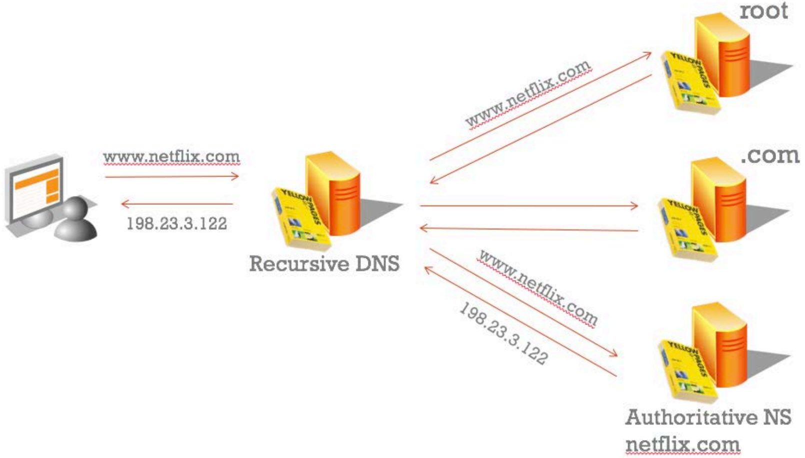
Agenda

- Introduction
  - DNS Data Exfiltration – What is it? How? Why?
  - Threat Landscape and Detection Challenges
- Detection Systems
  - Requirements and Key Principles
- Detection Systems’ Evaluation
  - How to assess if you are protected against DNS-based exfiltration?
- Summary and Conclusions

DNS – A Brief Background

DNS Protocol

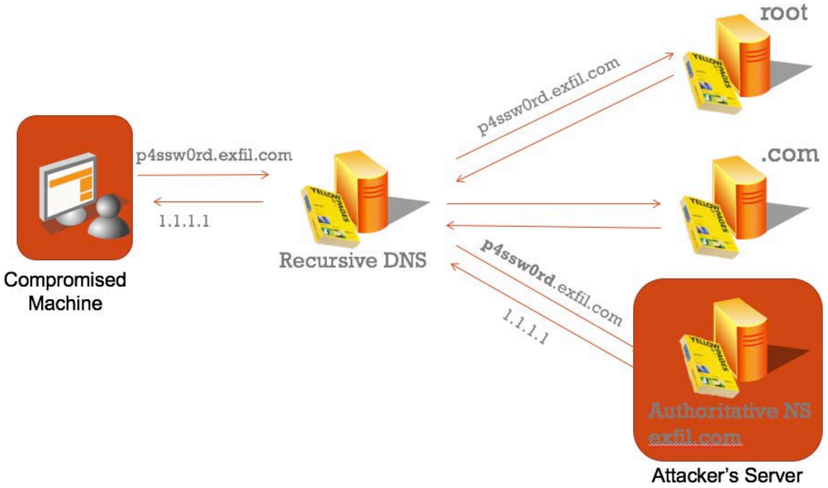
- DNS is mainly designed to resolve a hostname query to an IP address response
- The query is performed recursively, starting from the root DNS name servers until reaching the authoritative name server defined for queried domain.



DNS Exfiltration – How Does it Work?

DNS Data Exfiltration

- An attacker first sets-up his own authoritative name server
- Any compromised machine that queries that name server is a de-facto **established communication channel** between the machine and the name server.
- Extremely easy and cheap



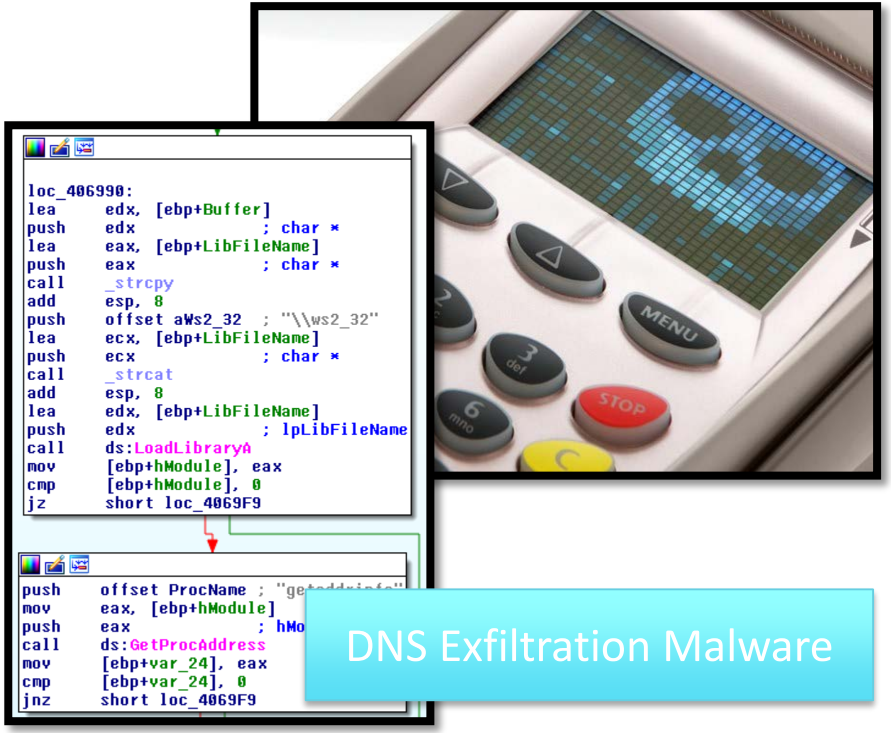
DNS Exfiltration – Attacker’s Motivation

- DNS is not an ideal covert channel:
  - Limited query size (up to 255 bytes)
  - Unreliable (order of messages is not guaranteed)

- However, DNS is:
  - A cornerstone of the Internet; available in almost every network
  - Rarely monitored compared to HTTP, FTP and e-mail protocols

DNS Exfiltration – Threat Landscape

DNS Tunneling Software



```
loc_406990:
lea      edx, [ebp+Buffer]
push     edx                  ; char *
lea      eax, [ebp+LibFileName]
push     eax                  ; char *
call     _strcpy
add      esp, 8
push     offset aWs2_32   ; "\\ws2_32"
lea      ecx, [ebp+LibFileName]
push     ecx                  ; char *
call     _strcat
add      esp, 8
lea      edx, [ebp+LibFileName]
push     edx                  ; lpLibFileName
call     ds:LoadLibraryA
mov      [ebp+hModule], eax
cmp      [ebp+hModule], 0
jz       short loc_4069F9
```

```
push     offset ProcName ; "getaddrinfo"
mov      eax, [ebp+hModule]
push     eax                  ; hMo
call     ds:GetProcAddress
mov      [ebp+var_24], eax
cmp      [ebp+var_24], 0
jnz      short loc_4069F9
```

DNS Exfiltration Malware

DNS Exfiltration – Threat Landscape

DNS Tunneling Software

- Common Usage
  - Web browsing over the DNS
  - Remote desktop protocols
- Examples:
  - Iodine
  - DNSCat
  - Dns2tcp

DNS Exfiltration Malware

- Common Usage
  - Sensitive data theft (e.g., passwords)
  - Command and control channel
- Examples:
  - FrameworkPOS (2014)
  - BernhardPOS (2015)
  - Win32.Backdoor.Denis (2017)

DNS Exfiltration – Detection Goals

- Any secure system should detect both:
  - DNS tunneling software
  - DNS exfiltration malware

- Isn’t the detection of both classes practically the same?
  - No. **The communication patterns of both classes are significantly different**.

DNS Exfiltration – Communication Patterns

DNS Tunneling Software

- Reliable
  - Frequent keep-alive messages
- Bi-directional and interactive
  - "Lengthy" responses
- Verbose
  - RDP / Web browsing with 255 byte messages requires a large number of messages

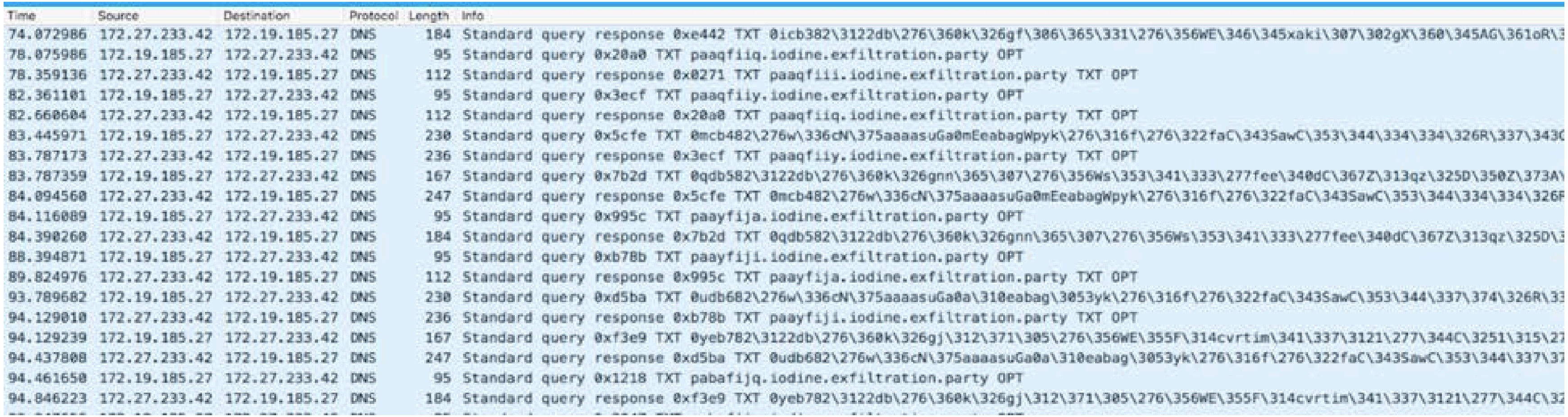
DNS Exfiltration Malware

- "Opportunistic" querying
  - A single credit card per swipe
- Possibly unidirectional
  - ACK response or no response
- Mostly unexpected
  - New attackers improve the ability to go "under the radar"

Iodine DNS Tunneling Traffic

4 Queries / Sec

Non-repeating Queries



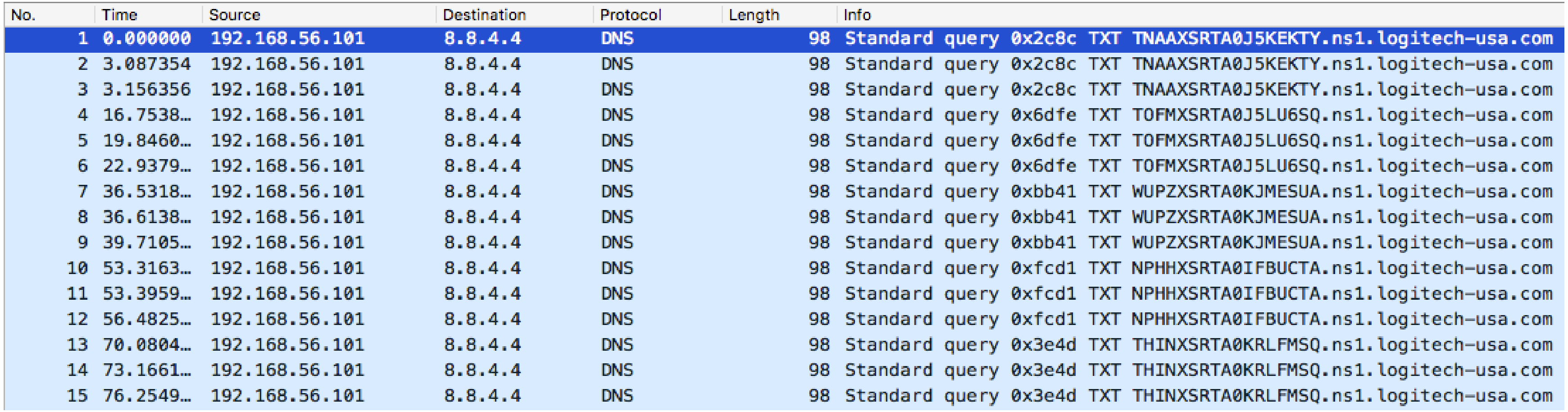
```
Time       Source         Destination    Protocol Length Info
74.072986  172.27.233.42  172.19.185.27  DNS      184 Standard query response 0xe442 TXT 0icb382\3122db\276\360k\326gf\306\365\331\276\356WE\346\345xaki\307\302gX\360\345AG\361oR\3
78.075986  172.19.185.27  172.27.233.42  DNS       95 Standard query 0x20a0 TXT paaqfiiq.iodine.exfiltration.party OPT
78.359136  172.27.233.42  172.19.185.27  DNS      112 Standard query response 0x0271 TXT paaqfiii.iodine.exfiltration.party TXT OPT
82.361101  172.19.185.27  172.27.233.42  DNS       95 Standard query 0x3ecf TXT paaqfiiy.iodine.exfiltration.party OPT
82.660604  172.27.233.42  172.19.185.27  DNS      112 Standard query response 0x20a0 TXT paaqfiiq.iodine.exfiltration.party TXT OPT
83.445971  172.19.185.27  172.27.233.42  DNS      230 Standard query 0x5cfe TXT 0mcb482\276w\336cN\375aaaasuGa0mEeabagWpyk\276\316f\276\322faC\343SawC\353\344\334\334\326R\337\343C
83.787173  172.27.233.42  172.19.185.27  DNS      236 Standard query response 0x3ecf TXT paaqfiiy.iodine.exfiltration.party TXT OPT
83.787359  172.19.185.27  172.27.233.42  DNS      167 Standard query 0x7b2d TXT 0qdb582\3122db\276\360k\326gnn\365\307\276\356Ws\353\341\333\277fee\340dC\367Z\313qz\325D\350Z\373A\
84.094560  172.27.233.42  172.19.185.27  DNS      247 Standard query response 0x5cfe TXT 0mcb482\276w\336cN\375aaaasuGa0mEeabagWpyk\276\316f\276\322faC\343SawC\353\344\334\334\326R
84.116089  172.19.185.27  172.27.233.42  DNS       95 Standard query 0x995c TXT paayfija.iodine.exfiltration.party OPT
84.390260  172.27.233.42  172.19.185.27  DNS      184 Standard query response 0x7b2d TXT 0qdb582\3122db\276\360k\326gnn\365\307\276\356Ws\353\341\333\277fee\340dC\367Z\313qz\325D\3
88.394871  172.19.185.27  172.27.233.42  DNS       95 Standard query 0xb78b TXT paayfiji.iodine.exfiltration.party OPT
89.824976  172.27.233.42  172.19.185.27  DNS      112 Standard query response 0x995c TXT paayfija.iodine.exfiltration.party TXT OPT
93.789682  172.19.185.27  172.27.233.42  DNS      230 Standard query 0xd5ba TXT 0udb682\276w\336cN\375aaaasuGa0a\310eabag\3053yk\276\316f\276\322faC\343SawC\353\344\337\374\326R\33
94.129010  172.27.233.42  172.19.185.27  DNS      236 Standard query response 0xb78b TXT paayfiji.iodine.exfiltration.party TXT OPT
94.129239  172.19.185.27  172.27.233.42  DNS      167 Standard query 0xf3e9 TXT 0yeb782\3122db\276\360k\326gj\312\371\305\276\356WE\355F\314cvrtim\341\337\3121\277\344C\3251\315\27
94.437808  172.27.233.42  172.19.185.27  DNS      247 Standard query response 0xd5ba TXT 0udb682\276w\336cN\375aaaasuGa0a\310eabag\3053yk\276\316f\276\322faC\343SawC\353\344\337\37
94.461650  172.19.185.27  172.27.233.42  DNS       95 Standard query 0x1218 TXT pabafijq.iodine.exfiltration.party OPT
94.846223  172.27.233.42  172.19.185.27  DNS      184 Standard query response 0xf3e9 TXT 0yeb782\3122db\276\360k\326gj\312\371\305\276\356WE\355F\314cvrtim\341\337\3121\277\344C\32
```

Longest Query is 248 characters

Wekby / Pisloader Malware Traffic

0.15 Queries / Sec

Queries are repeated



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.56.101	8.8.4.4	DNS	98	Standard query 0x2c8c TXT TNAAXSRTA0J5KEKTY.ns1.logitech-usa.com
2	3.087354	192.168.56.101	8.8.4.4	DNS	98	Standard query 0x2c8c TXT TNAAXSRTA0J5KEKTY.ns1.logitech-usa.com
3	3.156356	192.168.56.101	8.8.4.4	DNS	98	Standard query 0x2c8c TXT TNAAXSRTA0J5KEKTY.ns1.logitech-usa.com
4	16.7538…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0x6dfe TXT TOFMXSRTA0J5LU6SQ.ns1.logitech-usa.com
5	19.8460…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0x6dfe TXT TOFMXSRTA0J5LU6SQ.ns1.logitech-usa.com
6	22.9379…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0x6dfe TXT TOFMXSRTA0J5LU6SQ.ns1.logitech-usa.com
7	36.5318…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0xbb41 TXT WUPZXSRTA0KJMESUA.ns1.logitech-usa.com
8	36.6138…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0xbb41 TXT WUPZXSRTA0KJMESUA.ns1.logitech-usa.com
9	39.7105…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0xbb41 TXT WUPZXSRTA0KJMESUA.ns1.logitech-usa.com
10	53.3163…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0xfcd1 TXT NPHHXSRTA0IFBUCTA.ns1.logitech-usa.com
11	53.3959…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0xfcd1 TXT NPHHXSRTA0IFBUCTA.ns1.logitech-usa.com
12	56.4825…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0xfcd1 TXT NPHHXSRTA0IFBUCTA.ns1.logitech-usa.com
13	70.0804…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0x3e4d TXT THINXSRTA0KRLFMSQ.ns1.logitech-usa.com
14	73.1661…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0x3e4d TXT THINXSRTA0KRLFMSQ.ns1.logitech-usa.com
15	76.2549…	192.168.56.101	8.8.4.4	DNS	98	Standard query 0x3e4d TXT THINXSRTA0KRLFMSQ.ns1.logitech-usa.com

Longest Query is 98 characters

DNS Exfiltration - Midway

- The next part deals with detection of DNS tunneling and malware

- But first, what did we establish so far about DNS exfiltration?
  - Millions of credit cards stolen thus far
  - Popular attack due to an easy attacker setup and lesser security enforcement
  - Can be divided to two classes: DNS tunneling software and malware.
  - Capturing both is a challenge due to their different communication patterns

DNS EXFILTRATION DETECTION

Detection solutions for both DNS tunneling and malware

Key Considerations for Any Detection System

- Where does the solution resides?
  - Endpoint vs. Network Solutions Comparison

- What is the expected result?
  - Analysis Tool vs. Automatic Blocking

- How effective is the solution against new malware threats?
  - Manually Chosen Rules vs. Machine Learning
  - Actionable Reporting

Endpoint vs. Network Solutions

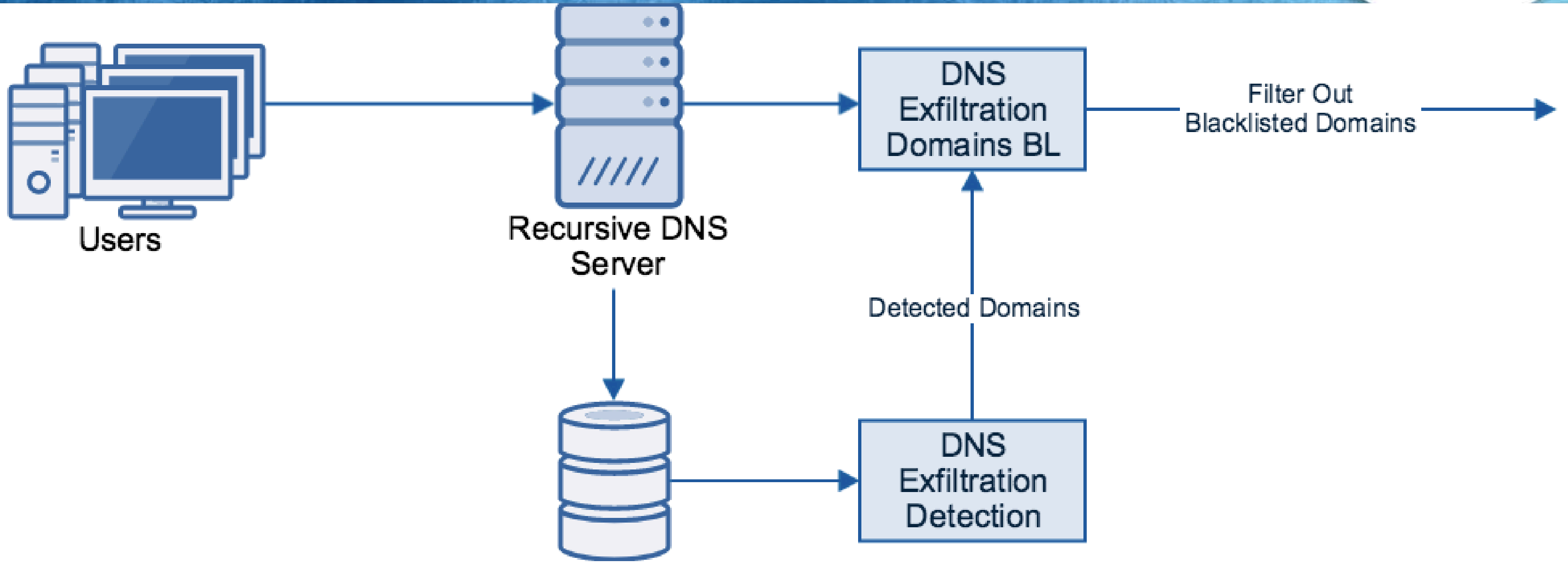
Endpoints Solutions

- Can leverage user context (e.g., running processes)

Network Solutions

- Can leverage global visibility (e.g., large scale bots, striking out widely-used services)
- Platform independent
- Ease of integration

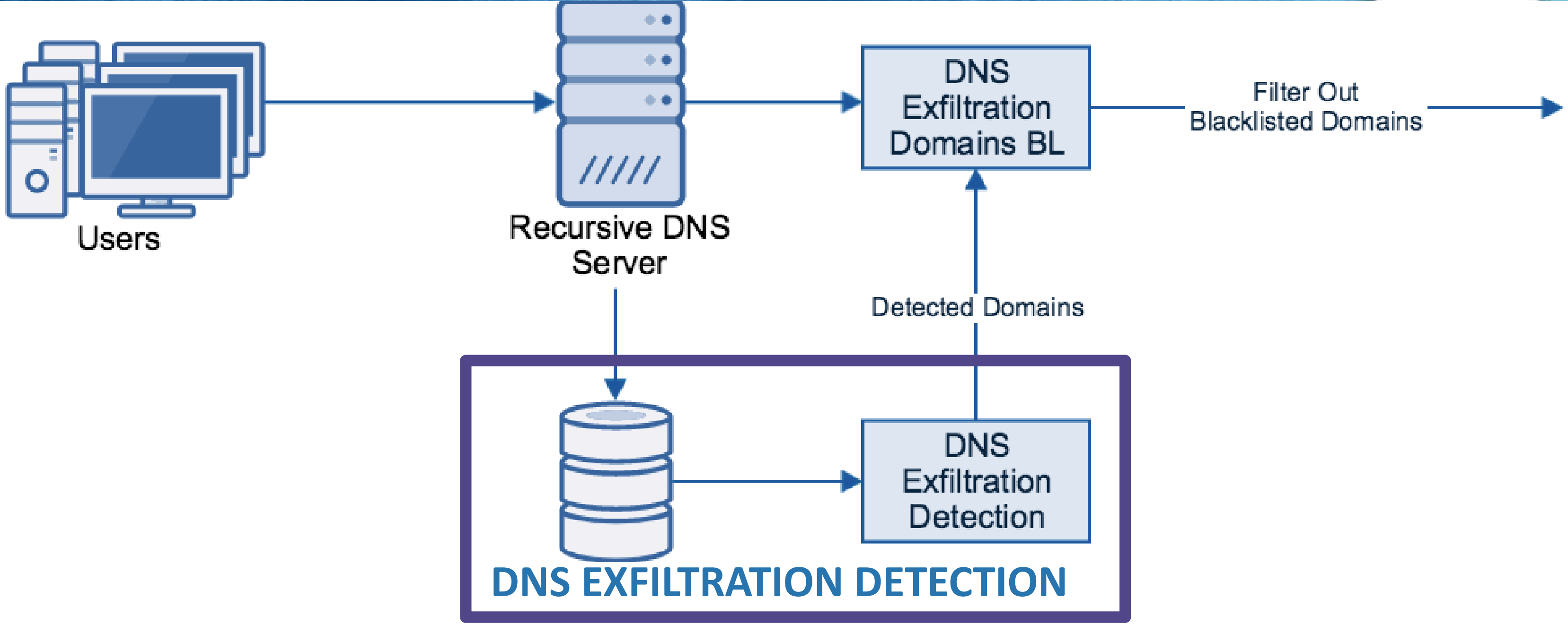
Network Solution Example


Users
Recursive DNS Server
DNS Exfiltration Domains BL
Filter Out Blacklisted Domains
Detected Domains
DNS Exfiltration Detection

DNS EXFILTRATION DETECTION

Recursive DNS logs are classified by a statistic model that decides what domains should be denied

Detection on the Recursive DNS Server


Users
Recursive DNS Server
DNS Exfiltration Domains BL
Filter Out Blacklisted Domains
Detected Domains
DNS Exfiltration Detection
DNS EXFILTRATION DETECTION

Recursive DNS logs are classified by a statistic model that decides what domains should be denied

Detection System’s Expected Results

Notification

- Useful for forensics and analysis
- Requires attendance

- Any object can be classified, e.g.,:
  - Users
  - Series of DNS queries

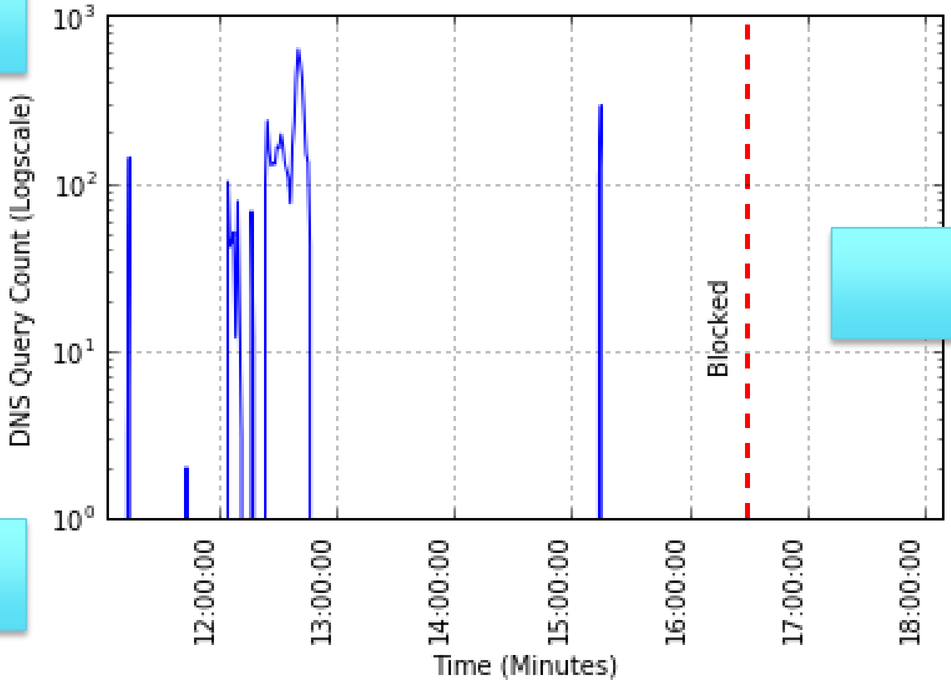
Automated Blocking

- Useful for unmanageable scale and sensitive-data networks

- Requires a block-able object, e.g.:
  - Domain
  - Specific process

Automated Blocking Example Report

A Bound on Data Loss



Blocking Latency

Allows Further Investigation

Effectiveness Against New Malware Threats

Rule-Set / Supervised Learning

- Rule-Set
  - No false alarms
  - Isn’t effective against new threats
- Supervised Learning
  - Learning from past examples
  - Limited to existing threats (if the number of training samples is insufficient)

Anomaly Detection

- Can predict when a new sample (e.g., domain) does not conforms to normal behavior
- Requires only normal sample
- Not completely free of false positive, but if effective against new threats

DNS Exfiltration Detection - Midway

- How can we evaluate a DNS exfiltration detection system?

- Before answering that, what did we discuss so far?
  - The residence of security and its implications (global visibility vs. user context)
  - Required compromises to act upon a threat (automated blocking)
  - Tradeoff between false positives and generalizing to new attacks

DNS EXFILTRATION DETECTION EVALUATION

How to make sure that the detection challenge is well solved?

Testing Your Security System

- Testing is better than trusting

- What’s important when testing your system?
  - DNS tunneling detection rate
  - DNS exfiltration malware detection rate
  - Latency until detection
  - Detailed reporting

What Should You Expect

- DNS tunneling detection rate
  - For a significant use (at least 10MB of bandwidth), expect 100% detection rate
  - Negligible amount of false alarms

- DNS exfiltration malware detection rate
  - Low survival rate (run up to 3 days and see if it’s eventually blocked).
  - Up to 10 false alarms per month

What Should You Expect

- Latency
  - Up to a few hours, but depends on how extensive is the use.
- Detailed reporting
  - Actionable (Who is the infected user? What domain was used?)
  - Allowing damage assessment

Testing Your Security System – DNS Tunneling

- Start with a DNS Tunneling Test

- Install a DNS tunneling client from https://your-freedom.net/
  - Cross-platform
  - Doesn't require a server-side setup

- Setup your web browser to use it as a proxy
  - User guide can be found on: https://your-freedom.net/index.php?id=doc
  - Consume at least 10MB of web browsing before giving up

Testing Your Security System - Malware

- Pisloader Malware
  - Point-of-Sale malware developed by the Wekby group

- Malware Sample
  - Can be downloaded on hybrid-analysis.com
  - SHA256: 456fffc256422ad667ca023d694494881baed1496a3067485d56ecc8fefbfaeb

- Fake C&C Server (by Palo Alto Networks):
  - https://github.com/pan-unit42/public_tools/blob/master/pisloader/wekby_dns.py

Testing Your Security System - Malware

- However, setting up "real malware" might be challenging
  - Mostly done by red-teams or security experts

- An easy-to-setup alternatives are open source Proofs-of-Concepts:
  - https://github.com/Arno0x/DNSExfiltrator
  - https://github.com/ytisf/PyExfil

- Guidelines for choosing an open source Proof-of-Concept:
  - No emulation of a reliable channel; queries are used almost entirely for payload
  - Easy setup for your operation system and technological stack
  - Control – bandwidth reporting, throttling (gap between consecutive messages), etc.

SUMMARY AND CONCLUSIONS

SUMMARY AND CONCLUSIONS

- DNS data exfiltration is major data leakage threat
  - Millions of stolen credit cards, credentials, etc.
  - Comprised of two main classes: DNS tunneling and malware
- A detection system should be chosen wisely
  - Demand automatic blocking, leveraging of global visibility and detailed reporting.
- Testing is better than trusting
  - With two simple tests, anyone can asses the quality of an organization’s detection systems

“Apply” Slide

- Next week you should:
  - Identify your organization’s defense mechanisms against DNS exfiltration
- In the first three months following this presentation you should:
  - Simulate a DNS tunnel from within your organization, and check if it’s blocked
  - Simulate our free DNS exfiltration malware test tool
- Within six months you should:
  - Choose a security system to detect DNS exfiltration according to your organization needs and risk assessment

QUESTIONS?