March 20, 2015

Dear Applicant:

RE: YOUR REQUEST FOR ACCESS TO INFORMATION UNDER PART II OF THE ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT – REQUEST #OCIO/001/2015

On March 13, 2015, the Office of the Chief Information Officer received your request for access to the following records:

"EWA Report delivered February 11, 2015 regarding the security breach of June 2013 and the OCIO handling of it."

I am pleased to inform you that your request for access to these records has been granted in part. Access to the remaining records, and/or information contained within the records, has been refused in accordance with the following exceptions to disclosure, as specified in the Access to Information and Protection of Privacy Act (the Act):

22(1)(L) - The head of a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to reveal the arrangements for the security of property or a system, including a building, a vehicle, a computer system or a communications system;

As required by subsection 7(2) of the Act, we have provided you with as much information as possible and only information that is excepted from disclosure, as well as information that is non-responsive to your request, has been severed. In accordance with your request for a copy of the records, the appropriate copies have been enclosed, as well as a summary of pages that have been redacted in their entirety from the request.

Section 43 of the Act provides that you may ask the Information and Privacy Commissioner to review this partial granting of access or you may appeal to the Supreme Court Trial Division. A request to the Information and Privacy Commissioner shall be made in writing within sixty days of the date of this letter or within a longer period that may be allowed by the Commissioner.

In the event that you choose to appeal to the Trial Division, you must do so within thirty days of the date of this letter; Section 60 of the Act sets out the process to be followed when filing such an appeal. You may also contact the Office of the Information and Privacy Commissioner who may decide to initiate an appeal pursuant to subsection 60(1.1). The address and contact information of the Information and Privacy Commissioner is as follows:

Office of the Information and Privacy Commissioner
34 Pippy Place, P. O. Box 13004, Station A
St. John's, NL A1B 3V8
Telephone: (709) 729-6309 or Facsimile: (709) 729-6500

P.O. Box 8700, St. John's, NL, Canada A1B 4J6  \( 709.729.2617 \)  \( 709.729.1464 \)
Please be advised that all general access ATIPP requests, including this final response letter and all responsive records, will be published to the Office of Public Engagement's website within seventy-two hours (if the request is sent to you electronically) or five days (if the request is sent to you via mail) of issuing this final response letter. Please note that personal information ATIPP requests are not posted online.

If you have any questions, please contact the Office of the Chief Information Officer’s ATIPP Coordinator, Ms. Tracey Goulding, at (709) 729-3896 or traceygoulding@gov.nl.ca.

Sincerely,

ELLEN MacDONALD
Chief Information Officer
INDEPENDENT SECURITY REVIEW

Document No. 1765-051-D001
Version Final 1.3, 11 February 2015

Prepared for:

Office of the Chief Information Officer
40 Higgins Line, Confederation Building
St. John’s, NL
A1B 4J6
Attention: Ms. Ellen MacDonald, Chief Information Officer

Prepared by:

Electronic Warfare Associates-Canada, Ltd.
139 Water Street Suite 601
St. John’s, NL
A1C 1B2
# TABLE OF CONTENTS

1 INTRODUCTION .................................................................................................................. 1
1.1 BACKGROUND .................................................................................................................. 1
1.2 PURPOSE .......................................................................................................................... 1
1.3 SCOPE .................................................................................................................................. 1
1.4 REFERENCES ..................................................................................................................... 2
1.5 DOCUMENT OVERVIEW ................................................................................................... 3

2 METHODOLOGY .................................................................................................................. 4

3 ANALYSIS .............................................................................................................................. 6
3.1 INCIDENT 1 ....................................................................................................................................... 7
3.2 INCIDENT 2 ................................................................................................................................... 10
3.3 ONGOING EVENTS .................................................................................................................. 13
3.4 RESPONSE TO [REDACTED] QUESTIONS ...................................................................... 14

4 CONCLUSIONS ...................................................................................................................... 16

ANNEX A - RELATED DOCUMENTS .......................................................................................... A-1
LIST OF TABLES

Table 1 Timeline of Events................................................................. 7
Independent Security Review

1 INTRODUCTION

1.1 BACKGROUND

On behalf of the Office of the Chief Information Officer (OCIO), EWA-Canada conducted an Independent Security Review (ISR) of events related to two IP addresses external to the Newfoundland and Labrador (GNL) networks that were suspected as being sources of malicious activity. The events related to these two IP addresses were believed to have occurred between June and July of 2013 and involved network communications between systems within the GNL and the two external IP addresses.

The events were described in two letters written by a former employee of OCIO. The first letter [1], dated 27 October 2013, was addressed to Premier Kathy Dunderdale. It described the alleged security incidents. The second letter [2] (email) dated 24 November 2014, was addressed to Tony Corneil, Minister of Service NL. It posed a series of questions related to the alleged security incidents. In both letters made claims that OCIO had improperly and inadequately handled the incidents, and that malicious activities related to these incidents were continuing.

1.2 PURPOSE

The objectives of the ISR were to:

a. make a determination as to whether either of the incidents were malicious in nature; and
b. if determined to be malicious, investigate whether the two events posed a current risk to the GNL network and/or its Information Technology (IT) assets.

1.3 SCOPE

The initial scope of the work was documented in an email from EWA-Canada, entitled “Letter for Independent Security Review”, dated 27 November 2014. OCIO instructed EWA-Canada to expand the scope as necessary in the course of the review to ensure that the events were fully investigated. The initial scope included:

a. meetings, telephone conversations, and email exchanges with people who had knowledge of the two events;
b. collection of available data such as data files, emails, event logs, and network traffic captures related to the two events;
c. examination of any hosts (systems) that might be implicated in the events;

---

1 The relevant time period was later determined to be February to September 2013.
d. analysis of the data obtained above in an effort to determine whether malicious activities actually occurred, or whether they were false alarms; and

e. a determination of whether OCIO's handling of the two events met industry accepted best practice for Incident Handling.

The timeframe for the investigation was subsequently expanded to cover the period of February to September 2013, and at OCIO's request, the questions posed in second letter were included in this report with answers provided to each question.

1.4 REFERENCES

The following provides a listing of relevant documents. The listing is limited to documents that are referenced in the body of the report or included as attachments. The attachments are provided as PDF documents separate from the report and labeled Annex1, Annex2, etc. corresponding to the numbering below. Note that this is not an exhaustive list. Many other computer files, emails and documents were reviewed during the course of the ISR.

Attachments

[9] GNL Support Desk, "Interaction SD343441 has been closed", 5 July 2013.

References


The "Security Group" consists of senior OCIO security staff. During the time of the events the members are believed to have included William Lorimer, Wayne Parsons, Gerard Dunphy, Jason Church and Basil James.
1.5 DOCUMENT OVERVIEW

The contents of the remaining sections of this document are as follows:

a. **Section 2.** This section describes the approach taken to conduct the work.

b. **Section 3.** This section presents the results of the work, including analysis of the events.

c. **Section 4.** This section provides conclusions derived from the review.
2 METHODOLOGY

The work included a review of all relevant data files, email, log files, and traffic captures that were made available by OCIO for review, as well as interviews with the people involved. The timeframe of information evaluated was initially believed to be June to July 2013, but was later expanded to the period of February 2013 to September 2013. The review was carried out during the period of 1 December 2014 to 28 January 2015.

Information examined by EWA-Canada included:

- OCIO staff email;
- support request tickets;
- firewall logs;
- DNS server logs;
- the file contents of [redacted] government network directory;
- the email archive associated with the [redacted] account;
- the contents of the laptop assigned to [redacted] while employed at OCIO;
- any other relevant data such as log and network traffic capture data related to the two events; and
- OCIO's past and current practices and procedures with respect to Incident Handling.

The following is a list of people with whom the events were discussed. These discussions included face to face meetings, telephone conversations, or email exchanges with:

- [redacted] formerly Senior Security Analyst, OCIO.
- Loretta Murphy (LM), Director-Operations, OCIO.
- Basil James (BJ), Senior Network Support Analyst, OCIO.
- Wayne Parsons (WP), Senior Security Analyst, OCIO.
- Phil White (PW), Network Operations Technical Services, OCIO.
- Gerard Dunphy (GD), Senior Security Analyst, OCIO.
- Alison Randell, Director Information Protection, OCIO.
- Tracey Goulding, IM Consultant (Information Protection), OCIO.
- Keith Budden, Manager of Operations for Service Delivery, OCIO.

The scope of the review was refined by EWA-Canada in terms of the specific time period, systems and individuals involved as information was collected and analysed. This was done to ensure that all relevant information was reviewed.

Once all of the available information provided by OCIO was analysed, EWA-Canada met with [redacted] on 22 December 2014. The purpose of the meeting was to discuss the events and to gather any further information that he could provide. He was made aware of the information gathered by EWA-Canada and our preliminary analysis of the events based on that information. He was then provided the opportunity to present his analysis of the events and any further supporting evidence he might have; to discuss EWA-Canada's
analysis of the events; and to pose any questions he might have regarding the investigation.
3 ANALYSIS

This section documents the analysis of the events surrounding the two incidents. The known details of each incident are described, followed by EWA-Canada's analysis of each incident.

The events in question were described by OCIO as being "two events" that occurred during June and July of 2013. In fact there were multiple, related events that occurred over a longer period of time. Data associated with these events spanned a time period of more than six months, from February to September 2013.

The common thread in these events and the associated data is that they relate to network communications between GNL computers located on the private GNL networks and two IP addresses that are external to the GNL private networks. The two IP addresses are:

- 22 (1)(L)

The events related to each of these IP addresses are described individually below. Events related to the first IP address will be referred to collectively as "Incident 1", while those events related to the second IP address will be referred to as "Incident 2". For each, a description of the events is presented followed by an analysis of the events related to that IP address.

The following table provides a timeline overview of the events.

<table>
<thead>
<tr>
<th>Incident</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident 1</td>
<td>Feb 2013</td>
<td>Firewall rules of February 2013 are found to already include a rule to block access to a domain name that resolved to When and why the rule was implemented is unknown.</td>
</tr>
<tr>
<td></td>
<td>13 Feb 2013</td>
<td>First discussion of potential Palevo botnet – See [3]</td>
</tr>
<tr>
<td></td>
<td>19 Apr 2013</td>
<td>Attempted traffic analysis by WL – See [5]</td>
</tr>
<tr>
<td></td>
<td>Apr 2013</td>
<td>The appliance no longer produces alerts on IP address</td>
</tr>
<tr>
<td></td>
<td>5 July 2013</td>
<td>Firewall change to block all traffic to put in place.</td>
</tr>
<tr>
<td></td>
<td>Jul-Sep 2013</td>
<td>WL continues to periodically gather traffic logs related to however there is no further email discussion with the OCIO Security team beyond that noted above.</td>
</tr>
<tr>
<td>Incident 2</td>
<td>19 Jun 2013</td>
<td>WL informs OCIO Security team about some research into covert channels over DNS -- See [6]</td>
</tr>
<tr>
<td>Incident</td>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>20 Jun 2013</td>
<td>WL requests analysis assistance re: suspicious DNS traffic - See [7]</td>
<td></td>
</tr>
<tr>
<td>25 Jun 2013</td>
<td>WL reports covert DNS channel - See [8]</td>
<td></td>
</tr>
<tr>
<td>26 Jun 2013</td>
<td>Firewall change to block traffic to [redacted] put in place</td>
<td></td>
</tr>
<tr>
<td>Jul-Sep 2013</td>
<td>WL continues to periodically gather traffic logs related to [redacted] however there is no further email discussion with the OCIO Security team beyond that noted above.</td>
<td></td>
</tr>
</tbody>
</table>

Table 1 Timeline of Events

3.1 INCIDENT 1

This incident involved internal GNL host computers that were causing security alerts by attempting to communicate with IP address [redacted] on [redacted]. The alerts occurred from February 2013 or earlier and continued through April 2013.

The alerts were being generated by GNL's [redacted] appliance, which is a network security management computer. This device scans network traffic moving in and out of GNL's computer networks searching for potentially malicious network traffic, and generates alerts upon detecting potentially malicious activity. These alerts are sent to the OCIO Security Group who is responsible for acting on the reported alerts.

It is important to note that these were unsuccessful connection attempts because at the earliest point in time covered by this investigation (February 2013) outgoing traffic to this IP was already being blocked by the external GNL firewall. OCIO staff were not able to provide EWA-Canada with any information on when or why this particular IP address had been blocked. A review of the firewall rules as they existed in February 2013 showed that the IP address was not explicitly blocked, which meant that the block was actually expressed as a domain name. While in February 2013 this domain name resolved to the IP address [redacted], that is not necessarily what the IP address was at the time the block was put in place. The assignment of domain name to IP address can change at any time. Due to a lack of documentation by OCIO it is impossible to determine today what the blocked domain name actually was, why the block was put in place, or whether IP address [redacted] was associated with it at the time the block was added to the firewall rules.

The first instance of IP address [redacted] being noted as a malicious IP is in an email [3] dated 2013-02-14 from GD to other members of the Security Group. It describes alerts
related to internal machines attempting communication with what were suspected to be Command and Control (C&C) servers that were part of a botnet\(^3\) known as Palevo\(^4\).

While multiple destination IPs were mentioned in the email, **[redacted]** is described as the most common. The email makes the following points in support of the determination that **[redacted]** is a Palevo C&C server. The text in italics is copied verbatim from the email.

- *This IP address hosts hundreds of thousands of domains.*
  (http://ip.robtex.com/[redacted] html)

- *This IP is still pointing to the Palevo C&C Botnet server.* 
  (https://paleovtacker.abuse.ch/?ipaddress=[redacted]). Palevo is a worm that spreads using instant messaging, P2P networks and removable drives (like USB sticks). It is being sold in underground forums like ZeuS.

- *Clean MX shows infrequent distribution of malware known as*
  (http://support.clean-mx.de/clean-
  mx/viruses.php?ip=[redacted]&sort=firstseen%20DESC ). This trojan will redirect the browser to malicious sites with unknown payloads.

- *VirusTotal shows detection ratio for this malware is 6/46*
  (https://www.virustotal.com/file/[redacted]/)

- **[redacted]** doesn't recognize this malware and thus does not have a signature for it.

- **[redacted]** doesn't recognize this malware and thus does not have a signature for it.

- *The three computers from yesterday were scanned and all came back clean.*

From this point forward this IP address was accepted by the Security Group as being a Command and Control (C&C) server for the Palevo botnet, and any traffic to this address was assumed to be infected hosts within GNL attempting to connect to the Palevo botnet C&C server. Emails related to new instances of GNL hosts attempting to communicate with this IP, as well as hosts previously restored being re-infected, continued to be discussed by the Security Group in emails through March and April 2013 [4].

---

\(^3\) A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, to perform malicious activities.

\(^4\) Palevo is a client component of the Mariposa botnet. The Mariposa botnet, discovered December 2008, is a botnet mainly involved in cyberscamming and denial of service attacks. A more detailed description of the botnet can be found at http://en.wikipedia.org/wiki/Mariposa_botnet.
On 19 April 2013 WL produced a report [5] that discussed traffic from GNL computers as well as failed DNS requests to it; however this report did not provide any answers to why this traffic was occurring. EWA-Canada’s assessment of this report is that there is nothing unusual or abnormal about any of the network traffic included in the report.

In April of 2013 stopped alerting on this IP address. This was because the vendor had stopped using the originating source of the alert, the Palevo Tracker website, as a source for malicious IP addresses.

Subsequent to this, on 5 July 2013 at WL’s request, all network traffic to and from IP address was blocked at the external firewall. This is noted in an email from the GNL Support Desk to WL [9].

**OCIO Response**

OCIO did not have a documented procedure for responding to malware infection alerts, however through a review of the available data and discussions with OCIO staff it was determined that the standard response to these events was to At that time, no traffic analysis or forensic examination were performed on any of the GNL computers involved.

A response based on current industry best practice would have included an analysis of network traffic for active sessions, combined with forensic analysis of the GNL hosts. In spite of the continuing traffic over a period of months involving many hosts, no such investigation was carried out.

**Analysis**

OCIO’s belief that connection attempts to IP address were related to Palevo malware infecting GNL hosts is flawed in several respects. These include:

- Firstly one must understand the nature of the web service that IP hosts. This IP is used as a domain name parking site to support redirection of users to other commercial websites. The domain names that resolve to this IP address are abandoned names that were once associated with legitimate or malware websites, but are now inactive. A domain name parking site may also host names that are misspellings of common web sites, from which a user may be redirected to some other website. The purpose of this is to generate advertising revenue by redirecting users to commercial sites. As a result, not much can be assumed about a host trying to connect to this IP based only on the connection attempt itself. Connection attempts to this IP could be anything from malicious software infections, to

---

5 For example the domain name "costo.ca", a misspelling of costco.ca, resolves to this IP address.
innocent misspellings of URLs typed in a user's browser, to attempts to connect to now defunct web sites.  

- Secondly, the tools used to scan suspect GNL machines did not turn up a single malware infection. Contrary to what is said in the email at [3], EWA-Canada’s research showed that both of these tools were able to detect the Palevo malware in February 2013. In addition to this, GD states in a later email [4] that can detect the Palevo malware. If the machines were infected then the malware should have been found. Additionally, OCIO staff when questioned stated that there wasn’t a single case of the Palevo worm being positively identified as having infected a GNL machine.

- Thirdly, if the events were caused by malware infections on the GNL hosts it could have been any sort of malware. While some domain names that point to this IP address may have been Palevo actors at one time, there are many thousands of other domain names that resolve to this IP. It would be wrong to make the assumption of Palevo infection simply based on destination IP address, but this is the only basis on which that assumption was made.

- Fourthly Palevo clients are known to communicate with their C&C servers on high UDP ports, not . Of course it’s possible that some variant could use this port, but this is at least unusual.

- Finally, in April of 2013 the appliance was reconfigured by the vendor to stop alerting on this IP address. Since this was the single source of the alerts related to IP there were no further incidents or discussions related to Palevo after this point in time.

Conclusion

After reviewing all of the available information, EWA-Canada did not identify any evidence that GNL internal hosts were infected with Palevo or any other malware during the time period covered by this review, and no evidence that they were ever able to successfully communicate with IP . It can therefore be said with confidence that the events in question did not result in any exfiltration of data from GNL hosts to IP address .

3.2 INCIDENT 2

The second incident involved internal GNL Domain Name Service (DNS) servers that were observed to be sending DNS requests to what was believed by OCIO to be a

---

6 https://www.abuse.ch/?p=3231
7 The Domain Name Service (DNS) is a global distributed database service that converts domain names to an IP address. For example a query for www.gov.nl.ca will return the IP address 209.128.28.18.
malicious host with IP address [redacted]. It was believed that there was a covert communication channel hidden in the DNS traffic to this host.

On 19 June 2013 WL sent an email [redacted] to the OCIO Security group stating that he had read an article [redacted] from 2011 that described covert communication channels over the DNS protocol. He stated that he hadn't seen any evidence of this but that they should keep a lookout for DNS traffic to "unusual" destinations when monitoring the alerts from the [redacted] appliance.

On the morning of Thursday, 20 June 2013 WL was asked by GD to monitor [redacted] as GD was busy with other tasks. At 4:55 PM WL emailed [redacted] the OCIO Security Group asking if there was a legitimate reason that the GNL DNS servers would be making DNS requests to [redacted]. A packet capture of a single DNS request and response pair was attached to that email. WL noted that the DNS traffic appeared to be normal, however he believed the IP address to be associated with malware in general and Palevo in particular. He therefore concluded the traffic was suspicious. He asked the OCIO Security Group whether this traffic should be investigated.

On the morning of Friday, 21 June 2013 GD replied that he was off for the day but that WP might be able to look at the traffic. As Monday was a holiday, there was no further discussion until Tuesday morning, 25 June.

On the morning of 25 June 2013 WL again emailed [redacted] the OCIO Security Group. He then stated that the DNS traffic to [redacted] was definitely a covert channel and recommended that the IP be blocked immediately. He stated the following as the reasoning behind his analysis of [redacted]:
- The destination IP is listed as a botnet C&C server on Palevo Tracker;
- The destination IP lights up like a Christmas tree on VirusTotal; and
- The URLs associated with the destination IP are all blocked by [redacted]

WP responded [redacted] by directing WL to arrange for the firewall to block outgoing network traffic to [redacted] as soon as possible. The block was put in place the next day.

The contents of WL's network home folder show that WL continued to periodically gather logs of traffic related to [redacted] through to September 2013, however there is no further discussion of this incident in email.

Analysis

WL's email of 25 June [redacted] makes three statements in support of the assertion that [redacted] is associated with malicious activity; however no evidence is provided to substantiate the claim of a covert channel. The three statements presented above that appear to support the assertion that the IP is malicious can be explained as follows:
"The destination IP is listed as a botnet C&C server on Palevo Tracker". This IP address serves the same purpose as the [redacted] IP address discussed in the previous section. It is a domain parking site that is linked to many thousands of inactive domain names. It is therefore almost inevitable that some of these domains will have been at some time associated with malware, and thus the IP address will be listed by malware tracking sites as being malicious.

"The destination IP lights up like a Christmas tree on VirusTotal". The same reasoning discussed above in relation to the first point can also be applied to this.

"The URLs associated with the destination IP are all blocked by [redacted]". The URLs in question did at one time point to other IP addresses that hosted malicious web sites. The domain names have since been deactivated and parked at this IP address, which does not host malicious web sites.

No evidence to support the existence of a covert channel is provided in that email [7].

One DNS request and response was captured by WL [7], and he stated at the time that it appeared to be normal but wasn't certain. In particular, he questioned the domain name that was being retrieved. The screenshots of the two DNS packets contained in that email were analysed by EWA-Canada and found to be normal. There was no indication of a covert channel in the traffic. The reverse DNS naming found in the packets, although uncommon, is normal. This form of naming is described in RFC 2317 [11].

[redacted] said that he did not see any other evidence to support his assertion of a covert channel. Additionally, he was unable to explain his assertion in [2] that the covert channel traffic was encrypted. EWA-Canada did not see any evidence of encrypted traffic in either of the two packets.

There is no evidence of any further investigation by OCIO into this DNS traffic. OCIO was unable to provide EWA-Canada with any other traffic captures related to this incident, and discussions with staff did not provide any additional information. There is no indication that anyone in the OCIO Security Group questioned WL's analysis or made any attempt to verify these claims.

Conclusion

As with the first event, the analysis of this traffic made assumptions about the traffic based solely on the reputation of the IP address and a misinterpretation of the DNS traffic. Existence of a covert DNS channel on the GNL networks is, in any case, unlikely. Exfiltration of data through such a covert channel would have resulted in a significant spike in DNS traffic that should have been detected; however no such spike was noted by anyone at GNL.
Based on the information reviewed there is no evidence that a covert channel existed within the DNS traffic described above. As a result, there is no evidence of exfiltration of any data from the GNL computers through a covert DNS channel.

3.3 ONGOING EVENTS

To determine whether any machines were still attempting to communicate with these two hosts, EWA-Canada had OCIO provide firewall logs that show all traffic blocked to these hosts. The logs were only available for the past three months as the logs are only kept for that period of time.

The analysis showed approximately 20 hosts attempting to connect to [redacted] and 40 attempting to connect to [redacted] over this 3 month period. In almost all cases there was only one attempt per host. In no case was there more than two. None of these computers were making the multiple ongoing connection attempts that would be expected for botnet infected hosts. That is not to say that none of these hosts are infected with malware - that could only be determined by detailed analysis of the host - but the traffic is not consistent with botnet infected hosts.

EWA-Canada also asked that DNS logging be enabled and that DNS queries to these IP addresses be provided for analysis. While this traffic is blocked at the GNL firewall, the DNS logs still provide the name of the site that was being looked up. These domain names were then accessed outside of GNL to determine where these names would lead if the traffic had been allowed. The following domain names were recorded in the logs and subsequently tested:

- costo.ca [redacted] - This domain name appears to be a mis-typing of costco.ca. The browser is redirected to an intermediary site that then redirects to alibaba.com. Alibaba.com is the Chinese version of amazon.com. This sort of redirection is common for these sites since the domain name owner generates revenue by redirecting dead and mis-typed domain names to commercial sites such as alibaba.com.

- www.cityorg-pdq.co.uk [redacted] - Redirects to a web site that offers to sell the domain name as well as referrals to commercial websites.

- alnera.eu [redacted] - Shows an empty web page on [redacted]

- jforjustice.co.uk [redacted] - Redirects to a commercial website.

Conclusion

This recent behaviour observed is consistent with the description of the two IP addresses as domain parking sites, as described in the preceding sections. Therefore it can be stated that there is no evidence that GNL is currently at risk due to any activity related to the two IP addresses that are the subjects of this report.
3.4 RESPONSE TO QUESTIONS

In an email [2] from [REDACTED] to Tony Cornell, dated 24 November 2014, [REDACTED] posed a series of questions related to these events. OCIO asked that these questions be addressed individually in the report. EWA-Canada has attempted to answer these questions where possible based on the analysis of the events as documented above and the scope of the investigation carried out by EWA-Canada. The questions in italics are copied verbatim from the email.

1. Given that the communication between the government network and the "botnet" control servers appears to have been encrypted, what technology did the OCIO use to determine that these messages did not contain any sensitive information?

The context for the question is missing, however if this is referring to the covert DNS channel then we can state that there is no evidence of a covert channel, therefore there were no messages, encrypted or not.

2. What technology did the OCIO use to analyse the content of messages that occurred far enough in the past that the relevant computer logs had been overwritten or otherwise destroyed.

It is unclear what messages are being referred to, however it is assumed that this question refers to the covert channel. If so, there are no messages to analyse since there is no evidence of a covert channel, encrypted or not.

3. Were the DNS servers themselves infected by a virus, or otherwise compromised?

There is no evidence of the DNS servers being compromised. EWA-Canada is unaware of any examination of the servers by OCIO at that time, however this is reasonable since there was never any indication that the DNS servers were compromised. Even if the covert DNS channel existed this would not involve compromise of the DNS servers.

4. How many government workstations were infected by the botnet virus/malware?

Within the scope of this investigation there is no reliable evidence to indicate that any GNL hosts were infected by botnet malware.

5. Which government workstations were infected? What government information did they have access to? How did the OCIO determine that this information was not compromised.

Within the scope of this investigation there is no reliable evidence to indicate that any GNL hosts were infected by botnet malware or that any data was exfiltrated as a result of any of the events in question.
6. **What steps were taken to clean any infected workstations and/or servers?**

None of the suspected machines were found to contain malware but as a precaution their storage media was erased and restored from a known good backup.

7. **Other than blocking the two known botnet controllers at the firewall, and terminating the employment of the IT security analyst who discovered the breach, was any other action taken by the OCIO to prevent recurrences?**

This ISR concluded that there was no breach; however OCIO staff stated in email that they now include network traffic analysis when alerted to similar events with further action dependant on the results of the analysis.

8. **How many of the infected computers were laptops or notebooks? Were any of them subsequently taken home or on the road and connected to networks outside the government firewall? If so, what assurances does the OCIO provide that they did not reconnect to botnet controllers?**

Within the scope of this investigation there is no reliable evidence to indicate that any GNL hosts were ever infected by botnet malware.

9. **Were are any other botnet control servers exploiting the covert channel?**

There is no evidence to support the existence of the covert channel.
4 CONCLUSIONS

Incident 1

Given the time that has elapsed from when the two incidents took place until the commencement of this ISR, much supporting forensics data was unavailable. This, combined with the absence of network traffic analysis and lack of detailed examination of the suspect GNL hosts at the time of these events, means that no absolute conclusions can be drawn with respect to the nature of the events related to IP address — 22 (1)(L)

However, there are reasonable explanations other than malware infection for the events described above, and there is considerable information that is inconsistent with OCIO’s belief that malware infected GNL hosts were communicating, or attempting to communicate, with Palevo Botnet controllers. It is therefore EWA-Canada's conclusion that the most likely explanation is that these hosts were not infected with the Palevo Botnet malware, or any other malware, and that the traffic seen was not malicious in nature.

Incident 2

With respect to the suspected covert communications channel through DNS, there is no evidence that a covert DNS channel ever existed within the GNL computer networks. The single DNS exchange captured by OCIO was normal DNS traffic in every respect. This network traffic was not encrypted, and there was no other evidence provided to support the existence of a covert channel through the GNL DNS servers, encrypted or otherwise. It is therefore EWA-Canada's conclusion that there was no covert DNS channel and therefore no exfiltration of GNL data to IP address — 22 (1)(L)

Residual Risks

The analysis of the events from February to September 2013, reinforced by analysis of current events as described in Section 3.3, lead to the conclusion that there is no evidence that GNL is currently at risk from any malicious activity related to the two IP addresses that are the subjects of this report.

Incident Response

GNL did not follow best practices in handling these incidents. Despite the belief that there was an ongoing and persistent malware infection over a period of several months in early 2013, and the belief that there was a covert communications channel allowing exfiltration of data in June of 2013, there was no attempt to do any in-depth analysis of the events. This analysis would have enabled OCIO to make a certain determination regarding infection, and if positive, to determine the source and method of infection. This would then have allowed them to take the necessary steps to remove the malware and prevent further infection. An effective Incident Handling process would have entirely avoided the mistaken assumptions of malware infections and the resulting costs of dealing with non-existent security events.
Other Considerations

The lack of documentation by OCIO on when or why the firewall change blocking was put in place brings into question the processes and procedures for firewall rule changes. GNL should ensure that sufficient information is recorded at the time of change, and that this information is preserved.

The process for making emergency changes to perimeter devices to control traffic flow is inadequate. Once the decision was made to block the IP address related to Incident 2, it took several days to get the firewall rule in place. While some mistakes were made in that case, it still would have taken days to implement the change since at that time firewall rule changes were only made twice weekly, even when changes were considered emergencies. Government should review current processes to ensure that there is a method whereby changes can be made in minutes rather than days in exceptional circumstances.

From discussions with OCIO staff, it is clear that there are difficulties in adequately dealing with potential security incidents due to the large volume of alerts.
ANNEX A
(Attachments)

Related Documents
Hon. Kathy Dunderdale
Premier of Newfoundland and Labrador

Dear Premier Dunderdale,

imagine going into a meeting to conduct trade negotiations, only to discover that your opposite counterparts were fully informed of your government's negotiating position due to a breach of security within the Government of Newfoundland and Labrador (GNL) computer network. Or imagine the political fallout if hackers broke into the GNL network, stole the names and addresses of Newfoundland and Labrador residents with legal narcotics prescriptions, and sold these addresses to drug dealers, thereby subjecting your constituents to home invasions. Imagine a computer in Eastern Europe exploiting a covert channel through a misconfigured firewall to launch a denial-of-service attack against the GNL network from the inside.

From February 11th until September 30th of this year, I was employed as a senior Information Technology (IT) security analyst, protecting the Government of Newfoundland and Labrador (GNL) computer network. I have over 35 years experience in the field of Information Technology security. I hold the Canadian Forces decoration (CD) and the Special Service Medal for service in the Canadian Armed Forces. I have been a Certified Information Systems Security Professional (CISSP) since January 2000, and I am also an Information Systems Security Architecture Professional (ISSAP). I was the lead security architect on the BOWMAN project, a billion-dollar military tactical command-and-control communications system handling classified military information for the British army. I hold two graduate degrees – a Master of Science in mathematical cryptography from Queen's University and a Doctor of Philosophy in computer science from the Centre for Information Security and Cryptography at the University of Calgary. So when I say that there are serious problems with the security of the GNL network, I know what I am talking about.

For example, in June - four months after I started work - I discovered a covert channel, a hidden and illicit communications channel that was allowing assets from within the GNL network to bypass the external firewall in order to communicate secretly with a known malicious site (a botnet command-and-control server) in eastern Europe. This channel had been operating, completely undetected, for several months at least; GNL firewall logs did not go far enough back to allow me to determine when the illegal traffic had begun, but there were indications that it had been ongoing at least since October 2012. I discovered this exploit late on Thursday June 20th, and sent e-mail warnings to the entire IT Security group at 4:55 pm on that day. Despite several e-mails from me to the entire IT Security group on Thursday, Friday, and Tuesday (Monday June 24th being a statutory holiday), it was not until the following Thursday night that the exploit was finally blocked at the firewall.
I subsequently discovered the same covert channel was being used by a different malicious server, this one located in New Zealand; this exploit was also successfully blocked. However, blocking those two malicious servers is only a band-aid solution. As of September 30th, despite the efforts of myself and another senior IT security analyst, the underlying vulnerability that allowed these exploits to compromise the security of the GNL network had not been fixed.

I was hired in February of this year as a senior Information Technology (IT) security analyst, to protect the Government of Newfoundland and Labrador (GNL) computer network. I could not, with a clear conscience, walk away knowing that a network I was responsible for was left in such a highly vulnerable state. There are many other security issues that need to be addressed urgently, which are not being given high priority. Although my employment with the Office of the Chief Information Officer was terminated on September 30, my professional code of conduct compels me to write this letter, in order to advise you that these serious deficiencies in the security of the GNL network still exist.

Cordially

Cc:
Hon. Tom Marshall, Q.C., President of Treasury Board, Newfoundland and Labrador
Hon. Dan Crummell, Minister Responsible for the Office of the Chief Information Officer, Newfoundland and Labrador
Hon. Dr. Darin King, Minister of Justice, Newfoundland and Labrador
David Norman, Deputy Minister for Service NL
Robert P. Johnston, Chief of Police, Royal Newfoundland Constabulary
David Brazil, MHA Conception Bay East/Bell Island
V. Randall J. Earle Q.C., O’Dea Earle
Dear Minister,

I am very pleased that you have asked for an external investigation into the OCIO’s handling of the security breaches I discovered last June. Of course, a cynic might question why the OCIO have been tasked to choose their own auditors. In the interests of “due diligence”, perhaps you will stipulate that the “independent IT security firm” be from outside the province, rather than a local firm that currently does a large volume of business with the OCIO.

Regardless of which firm is selected to investigate, I am providing you with a number of questions that their findings, at minimum, must answer.

1. Given that the communication between the government network and the “botnet” control servers appears to have been encrypted, what technology did the OCIO use to determine that these messages did not contain any sensitive information?

2. What technology did the OCIO use to analyze the content of messages that occurred far enough in the past that the relevant computer logs had been over-written or otherwise destroyed?

3. Were the DNS servers themselves infected by a virus, or otherwise compromised?

4. How many government workstations were infected by the botnet virus/malware?

5. Which government workstations were infected? What government information did they have access to? How did the OCIO determine that this information was not compromised?

6. What steps were taken to clean any infected workstations and/or servers?
7. Other than blocking the two known botnet controllers at the firewall, and terminating the employment of the IT security analyst who discovered the breach, was any other action taken by the OCIO to prevent recurrences?

8. How many of the infected computers were laptops or notebooks? Were any of them subsequently taken home or on the road and connected to networks outside the government firewall? If so, what assurances does the OCIO provide that they did not reconnect to the botnet controllers?

9. Were/are any other botnet control servers exploiting the covert channel?

I understand that cabinet ministers are not necessarily technical, and may feel that they must rely on the expertise of their staff. However, waiting for a disaster to occur and then blaming your subordinates for misleading you is not leadership, and relying on the competence of staff whose competence is being questioned is a fool’s approach.

Thank you for your attention to this matter.

Sincerely
From: Dunphy, Gerard
Sent: Thursday, February 14, 2013 4:43 PM
To: Parsons, Wayne; White, Philip; Lorimer, William
Cc: Church, Jason; Murphy, Loretta
Subject: RE: Botnet Traffic

Wayne, Phil

We've had several more instances of C&C botnet communications as of this morning:

I had a look at the most popular IP here and have determined the following:

- This IP address hosts hundreds of thousands of domains. ([http://ip.robtex.com/](http://ip.robtex.com/))
- This IP is still pointing to the Palevo C&C Botnet server ([https://palevotrack.abuse.ch/?ipaddress=](https://palevotrack.abuse.ch/?ipaddress=)). Palevo is a worm that spreads using instant messaging, P2P networks and removable drives (like USB sticks). It is being sold in underground forums like ZeuS.
- Clean MX shows infrequent distribution of malware known as ([http://support.cleannx.de/clean-mx/viruses.php?ip=](http://support.cleannx.de/clean-mx/viruses.php?ip=) &sort=firstseen%20DESC). This trojan will redirect the browser to malicious sites with unknown payloads.
- VirusTotal shows detection ratio for this malware is 6/46 ([https://www.virustotal.com/file/](https://www.virustotal.com/file/))
- doesn't recognize this malware and thus does not have a signature for it.
- doesn't recognize this malware and thus does not have a signature for it.
- The three computers from yesterday were scanned and all came back clean.

In summary, there is supporting evidence to indicate this is a viable threat. Considering this information I think the safest approach is to If you agree, can you give Keith Budden a head's up that I will issue SM7 tasks to Please let me know either way.

(P.S. I will also look into the other IP's in this list and determine the threat.)
Thanks,

Gerard

From: Dunphy, Gerard  
Sent: Wednesday, February 13, 2013 10:25 AM  
To: Parsons, Wayne; White, Philip (PhilipWhite@gov.nl.ca); Lorimer, William  
Cc: Church, Jason; Loretta Murphy  
Subject: Botnet Traffic

Guys,

We're seeing an increase in botnet traffic lately. A few each day this week followed by this morning, we have 8 computers attempting to communicate with a C&C botnet (ShadowServer) known for malware distribution. Note the times are mere seconds apart.  

22 (1)(L)

Gerard
Will,

Virus Total also indicates currently infected site. 

Gerard

From: Lorimer, William 
Sent: Wednesday, March 20, 2013 3:10 PM 
To: Dunphy, Gerard; Parsons, Wayne 
Subject: Palevo Trojan infection - Non-Responsive

Another suspected Palevo botnet Trojan, 

Dst: (still active according to https://palevotracker.abuse.ch/)

The traffic is basically identical to the other suspected botnet infections.

Will
Wayne,

As these have been out for a while now I think the time has come to re-examine our remediation process. I’ve confirmed [blacked out] has signatures for Zeus and Palevo. Also, bot communications are being blocked at the firewall.

Thoughts?

Gerard

Gentlemen,

Two issues

1. This is the fifth machine in the last two weeks that has been hit with the zues trojan. the really interesting thing is that all 5 machines are [blacked out] 22 (1)(L)

   Have you noticed that this "virus" on other types of machines.

   Also we are getting conflicting methods as to how to deal with the threat.

I ask this because it is really taxing and resource intensive to [blacked out] 22 (1)(L)

regards

[blacked out] Non-Responsive
We need to analyze the data. We will discuss in tomorrow team meeting.

Cheers

Wayne

Hi, Wayne

Some further info on this asset:

I flagged the latest offense in [redacted] and I have been monitoring it. I just exported the list of events to an Excel spreadsheet (see attached for the data export).

Summary:
From: Parsons, Wayne
Sent: Monday, March 25, 2013 10:49 AM
To: Lorimer, William; Dunphy, Gerard
Subject: RE: IM243129 - asset [REDACTED] apparently infected AGAIN?

Let it with me until after lunch. I will discuss with Jason.

I will advise the next steps.

Cheers

Wayne

From: Lorimer, William
Sent: Monday, March 25, 2013 10:40 AM
To: Parsons, Wayne; Dunphy, Gerard
Subject: RE: IM243129 - asset [REDACTED] apparently infected AGAIN?

Wayne, Gerard

The following asset [REDACTED] was flagged twice and [REDACTED]

According to [REDACTED] this asset has been communicating with the same Palevo server in Australia, starting again on 2013-03-22 18:40:22 - 2 days after John Evoy [REDACTED]

The asset attempted to contact the suspect IP for a period of 1d 9h 21m 26s.

I confirmed this is the same asset [REDACTED] on Wednesday March 20 from the SM7 ticket:

IM243129:

The Australian server is still listed as an active botnet C&C by the following sites:


Palevo Tracker – https://paleotrack.abuse.ch/?ipaddress= [REDACTED], 4 URLs in the green, last seen 2013-03-25 12:32:41 (UTC) (i.e. within the last half hour).
For what it's worth, MyWOT also reports this site as having a Very Poor reputation in 4 out of 4 categories: 

I propose that we have John Evoy

I'd also like to know if this is the only machine that these staff members are using, or are there other machines accessible? If there are other machines, then why would this be the only one affected?

Any thoughts/suggestions?

Will

From: Evoy, John E.
Sent: Wednesday, March 20, 2013 3:35 PM
To: Parsons, Wayne; Dunphy, Gerard; Lorimer, William
Subject: IM243129

The asset listed in this ticket [REDACTED] However this is the second time in as many weeks that this PC has reported the same virus. I was speaking with William on this and he asked for an email regarding this ticket to create a paper trail in case this asset gets the virus again.

John Evoy | Computer Support Specialist
Office of the Chief Information Officer

709 729-5752 (t) | 709 729-3445 (f) | jevoy@gov.nl.ca
From: Lorimer, William  
Sent: Monday, April 08, 2013 11:34 AM  
To: Church, Jason  
Subject: RE: Activities Report

Jason

Here is mine.

Began reviewing activity for suspected botnet Command & Control IP address using

Will

From: Church, Jason  
Sent: Monday, April 08, 2013 8:58 AM  
To: OCIO-OPS-NetOps  
Subject: Activities Report
Hello, everyone.

Attached is a document containing my findings on using [BLANK] to analyse traffic. I tried working through Gerard’s document, but I haven’t been able to get the Console set up properly on my machine so I’ve been limited in my ability to follow Gerard’s instructions. However, I was able to figure out how to use the web-based interface to do some basic traffic analysis, as described in the attached document.

Will Lorimer
After some trial and error and experimentation, I was able to start performing an analysis of some suspected botnet traffic.

By filtering on IP, I confirmed that there has been some traffic to/from this site, even though this is no longer being reported in


GNL IP asset is continuing to attempt communication with this server at odd times. This is the asset that has already been

Other assets are also attempting to communicate with this server; for example:

This is just a sampling of traffic to/from this server.
I'll keep working on this as time permits, at least in order to familiarize myself with the working of the technology.
All

In the course of doing some research, I came across this paper from 2011. It describes how infected machines, even if they are completely blocked from using the Internet by the firewall(s), can use the corporate DNS servers as proxies to establish a covert channel with a malicious external site – e.g. a Botnet C&C.

When I typed this command into [redacted], this is what I got back: 22 (1)(L)

So from a preliminary inspection, the GNL network appears to be vulnerable to this type of covert channel.

I've seen no evidence that any such communication is taking place but we should be aware that it might be and perhaps keep a lookout for any DNS/[redacted] traffic to "unusual" destinations when we're monitoring the IDPS.

Will
DNS as a Covert Channel Within Protected Networks

Author
Seth Bromberger, Co-Principal Investigator, NESCO

Document Number
WP2011-01-01

Revision
1.1

Publication Date
25 January 2011

Acknowledgement / Disclaimer
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000516.

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.
I. Overview

Critical information relating to company operations exists within the electric sector on both control/operations and business networks. While most attempts by malicious actors to exfiltrate this data have required the ability to establish inbound or outbound connections to these networks, there are other methods of exfiltration that do not rely on direct connections that are generally blocked by perimeter security devices. Exfiltration of data via Domain Name System (DNS) queries is a method of breaching the confidentiality of company information that is commonly available, hard to detect, and can provide indirect command and control (C2) channels between an attacker and compromised hosts.

This whitepaper discusses ways to detect DNS exfiltration attempts based on current known methods, and provides recommendations for mitigation of this exposure.

To restate: The DNS exfiltration techniques described below do not require direct connectivity to any external resource from the target machine.

II. Technical Summary

- Malicious software is known to exfiltrate confidential data and establish command-and-control channels using DNS A, SRV, and TXT queries.
- The communications channel can be established on any network device whose configured DNS servers enable resolution of untrusted or external hosts. A quick check: if resolution of “exfilt-test.energysec.org” returns 10.0.0.9, establishment of a communications channel using DNS is possible from the tested host.
- Detection of this communications channel involves inspection of DNS queries and responses. Indicators are listed below.
- Mitigation methods can include isolating DNS servers on protected networks so that they do not forward queries to untrusted or less protected networks or devices.
- NESCO staff are available to provide assistance in the event you detect anomalous DNS traffic. We can help get you in touch with other organizations with nonattributable communications where appropriate.

III. Description of Issue

Exfiltration of data from control systems and business networks can put an entire organization at risk. Whether the information relates to business intelligence, operations plans, or lists of critical assets, the unauthorized disclosure of data can pose a great risk to an organization’s continuity of operations.

Most methods of remotely-initiated data exfiltration rely on two components: the compromise of a target host, and the interconnectedness of that host to the attacker’s network in order to effect the transfer of sensitive data from the target machine. In response to these requirements, many operational networks are isolated from public networks such as the Internet, and have well-defined and documented interconnections to other non-public networks (such as the organization’s business or general user network).

Even with a well-defined set of interfaces to other networks, all networks require some set of common infrastructure services in order to function normally. Among those services is network name resolution, commonly implemented using the Domain Name System (DNS). It is via DNS that common names of servers and other network devices are associated with the Internet Protocol (IP) network addresses that are used to establish connectivity among communicating
hosts. Without this service, IP-based communications are often restricted to using numeric IP addresses to establish connectivity. Using IP addresses in this manner has impacts on network and service availability, and makes network reconfiguration and maintenance more difficult.

The process by which most DNS resolution occurs is via query forwarding: that is, if a DNS nameserver is not authoritative for the underlying domain, it will relay the query to other nameservers that either are authoritative for the domain or can further relay the query. In this way, the IP addresses for internet hosts such as www.google.com can be resolved by hosts within a protected network: the local DNS servers are queried first; since they are not authoritative for google.com, they will relay the query to a set of servers that can either query the authoritative nameservers or can pass the query to a server that can further relay the query. This allows arbitrary name resolution by hosts without requiring a direct connection to the set of nameservers that might hold the data for the destinations being queried.

A full description of DNS forwarding is outside the scope of this paper. Please see the appendix for further references.

The act of relaying DNS queries from secure systems to arbitrary internet-based nameservers forms the basis of this uncontrolled data channel. Consider a target host that meets condition 1: it has been compromised by some malicious software. Even if we assume that connections to public networks are not allowed, if the target host is able to resolve arbitrary domain names, data exfiltration is possible via forwarded DNS queries, as shown in the following example.
Setup: A malicious application on the target host is designed to transfer the contents of a specific file ("confidential.doc") to an adversary who controls a public internet server and has control of a domain name ("badguy.com"). The malicious application takes the contents of the confidential.doc ("ultra-secret stuff") and prepends it to the "badguy.com" domain ("ultra-secret.stuff.badguy.com") and then requests name resolution for this domain name. (In most cases, the data are typically encoded or encrypted prior to prepending to the adversary's domain.)

Steps 1 - 3: The target host's primary nameserver receives this request, determines that it is not authoritative for "badguy.com", and forwards the request through a series of internal and external nameservers where it eventually reaches "nameserver.badguy.com", the nameserver that is authoritative for "badguy.com" and is under the adversary's control.

Steps 4 - 5: "nameserver.badguy.com" receives and logs the "ultra-secret.stuff.badguy.com" request. The adversary now has the target's confidential data. In addition, the adversary now has the opportunity to return command and control data to the target via the expected response: an IP address. The malicious application could interpret specific IP address responses as instructions to perform other activity, such as erasing or modifying data, interfering with computer operation, or exfiltrating other data.

IV. Indicators

Testing to determine whether such an attack is feasible is very straightforward. Both UNIX and Windows systems have a command called "nslookup" which can be used to test DNS resolution. NESCO has set up a test domain name that can be used to determine whether DNS forwarding is enabled for a given device/network. At a command prompt, if "nslookup exfiltr-test.energysec.org" returns an IP address of 10.0.0.10, then externally-forwarded name resolution is enabled from that system and, if the system were to be infected by malicious
software that uses the techniques described above, exfiltration and C2 access would be successful.

Determining whether any systems are actually exfiltrating data via nameserver queries is a bit more difficult and requires access to the corporate nameservers’ query logs (which may not be enabled by default). Note that in many cases, encryption or encoding of the query data makes it difficult to analyze the queries themselves for the presence of confidential or control information.

Current known attacks utilizing DNS exfiltration include one or more of the following characteristics:

- DNS name lookups that have multiple levels (a.b.c....n.domain.com) where a,b,c,...n are composed of hexadecimal strings (e.g., e04fde587a1.f6c7.example.com)
- DNS name lookups as described above, where the cumulative length of the third and higher-level names (a.b.c....n) exceeds 40 bytes
- Multiple DNS name lookups to non-obvious or foreign domains (e.g., 4c7a.obscure.com, 1a6d.some.site.cn)
- Multiple DNS name lookups to several non-obvious or foreign domains within a short timespan
- DNS TXT or SRV record queries to non-obvious or foreign domains
- DNS responses that include loopback or RFC1918 address space (e.g., a response to an external DNS query of any address in the 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, or 192.168/16 netblocks) - these can indicate C2 activity as described above.
- Multiple DNS queries to non-obvious or foreign domains occurring outside of normal business hours, including weekends
- DNS queries to Dynamic DNS service providers (e.g., dyndns and xname)
- DNS queries that are not followed by a proxied request for connection (such as HTTP, FTP, or other expected data transfer)

V. Mitigation

To prevent DNS exfiltration from a protected network, ensure that DNS queries are not relayed outside the trusted perimeter. This will prevent any information being leaked via DNS to untrusted hosts.

To detect DNS exfiltration, evaluation of namequery network traffic is required. The easiest way to accomplish this is to enable query logging on nameservers; however, the servers can quickly become overloaded with logging data if they are not sufficiently provisioned to handle this extra load. Network sensors that can capture DNS traffic could also be used. Implementation of network sensors is more difficult, but can yield better results as analysis of inbound and outbound DNS traffic is generally easier.

Correlation of DNS queries to other proxy logs to determine whether the queries were the result of legitimate service access is also very important. Outbound connection logs, including firewall and other perimeter control devices, should be monitored in conjunction with DNS queries, and any DNS query that does not result in a proxied outbound connection request should be investigated.

VI. What to do if you detect this activity

If you detect suspicious DNS traffic on your networks, your company’s computer incident response and forensics plans should be activated. NESCO is here to help: if your organization
needs assistance in interpreting logs or in contacting other incident response organizations, please reach out to us. Our contact information is listed below.

VII. Conclusion

Exfiltration of sensitive information and command and control of critical systems using DNS as a covert communications channel is no longer relegated to the class of theoretical attacks. However, while attacks against utility systems using DNS exfiltration have been reported, the extent to which the compromises resulted in disclosure of confidential data is unknown due to encryption of the payloads. It is therefore important to assume that any evidence of DNS exfiltration in a sensitive environment has targeted confidential information and has resulted in full command and control of the affected devices.

VIII. Appendix and Further Reading

Hi, all

Is there a legitimate reason why our DNS servers should be regularly communicating with a server in the Czech republic that is not only on the Palevo tracker list, but has a lengthy “rap sheet” on VirusTotal (https://www.virustotal.com/en/ip-address/)?

The traffic appears to be legitimate DNS queries; a PTR query for a reverse DNS lookup on IP and a type A response; however, DNSTools indicates that exists in the UK. However, there’s no indication on DNSTools that a exists; although that may not mean anything, the subnet exists and it DOES show up in DNSTools. Also, the response doesn’t really resolve the IP address to a name; it just returns the in-addr.arpa entry.

When I checked using I was able to track traffic to this server as far back as April 20. In doing research, I came across a number of papers and web pages describing how DNS servers are being used as proxies to create covert channels through firewalls.

Is this traffic something that needs to be followed up with further investigation?

Thanks.

Will
Church, Jason

June 25, 2013 11:26 AM

James, Basil

Lorimer, William; Parsons, Wayne

RE: Covert channel through GNL external firewall

Basil lets process this to ensure this gets implemented tonight please.

Jason Church

Parsons, Wayne

From: Parsons, Wayne

Sent: Tuesday, June 25, 2013 11:19 AM

To: Lorimer, William; James, Basil

Cc: Church, Jason

Subject: RE: Covert channel through GNL external firewall

Will You will need to follow up with Basil, Jason and change management to ensure this gets implemented tonight.

Cheers

Wayne

Lorimer, William

From: Lorimer, William

Sent: Tuesday, June 25, 2013 10:22 AM

To: Parsons, Wayne; James, Basil

Cc: Church, Jason

Subject: RE: Covert channel through GNL external firewall

Wayne

I raised SD340500, escalated it to Network OPS as change C144218, and attached firewall change request 'C144218 - Emergency blocking of malicious site.docx' to the change request. C144218 is currently assigned to Basil James.

Please let me know if there is anything more I need to do with regard to this change request.

Meanwhile, I will investigate to see what other assets have been communicating with this external site.

Thanks.

Will

Parsons, Wayne

From: Parsons, Wayne

Sent: Tuesday, June 25, 2013 9:46 AM

To: Lorimer, William; Church, Jason
Will,

Please arrange to have this IP blocked ASAP. Work with network operations to determine if this can be completed tonight.

This will be an emergency change.

Cheers

Wayne

From: Lorimer, William
Sent: Tuesday, June 25, 2013 9:17 AM
To: Church, Jason
Cc: OCIO Security
Subject: Covert channel through GNL external firewall

Jason

Something needs to be done about this. This is a covert channel using our DNS servers as proxies to tunnel information of some sort through the firewall.

1. The destination IP is listed as a botnet C&C server on Palevo Tracker;  
2. The destination IP lights up like a Christmas tree on VirusTotal;  
3. The URLs associated with the destination IP are all blocked by [redacted]

This is not a site that any GNL asset, let alone our [redacted] DNS servers, should be communicating with.

My recommendation is that this IP address be blocked immediately at the firewall, both inbound and outbound, on all ports. (Note: [redacted] does not block IP addresses, it only blocks URLs.) We also need to launch an investigation to find out which assets are using the DNS servers to communicate with this controller.

This isn’t without risk; there’s always a possibility that the infected assets will do something overtly malicious (e.g. a logic bomb) if communication with the mother ship is cut off; however, this communication has been going on for at least two months before I discovered it, and probably much longer than that. I believe the sooner we cut it off, the better.

We should also consider reporting this to CCIRC, but that’s a management call.

Will Lorimer
Interaction SD343441 has been closed.
** Please do not reply to this email message **

Dear Sir/Madam,
Interaction SD343441 has been closed with the following details:

**Title:** Emergency blocking of IP "********"  
**Description:** Add IP "********"  
  IP "********" is listed on Palevo Tracker and has multiple recent malware activities noted on VirusTotal as recently as 2013-07-03 09:32:01

**Description of Solution:** Related Change C145544 closed.

reject

**** **There are no other related records. Interaction closed by Change C145544**

If you have any queries you can always contact the Service Desk.

Kind regards,
OCIO Service Desk (servicedesk@gov.nl.ca)
<table>
<thead>
<tr>
<th>Page #</th>
<th>Reason for Redaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>37-47; 49-52; 61-62</td>
<td>s.22(1)(L)</td>
</tr>
</tbody>
</table>