Sword & Shield
ENTERPRISE SECURITY
Your Partner for a Secure Future

May 8, 2018

Root Cause Analysis

Knox-County-Election-Web site-5-8-2018

Prepared for: KNOX COUNTY TENNESSEE

PROTECT DETECT RESPOND

Table of Contents

Contact Information

Vice President of Services
Fred Cobb
Sword & Shield Enterprise Security
fcobb@swordshield.com

Enterprise Solutions Consultant
Scott Partelow
Sword & Shield Enterprise Security
sep@swordshield.com

Account Manager
Mike Mangione
Sword & Shield Enterprise Security
mam@swordshield.com

Overview

Knox County Tennessee contracted Sword & Shield Enterprise Security Inc. (Sword & Shield) to conduct a Root Cause Analysis. The objective of the analysis was to ascertain the root cause of a Web site outage on May 1, 2018. Logs from the Knox County firewall, Proxy server and Web server were given to Sword & Shield for event correlation and review.

A summary of the key findings for May 1st is listed below:

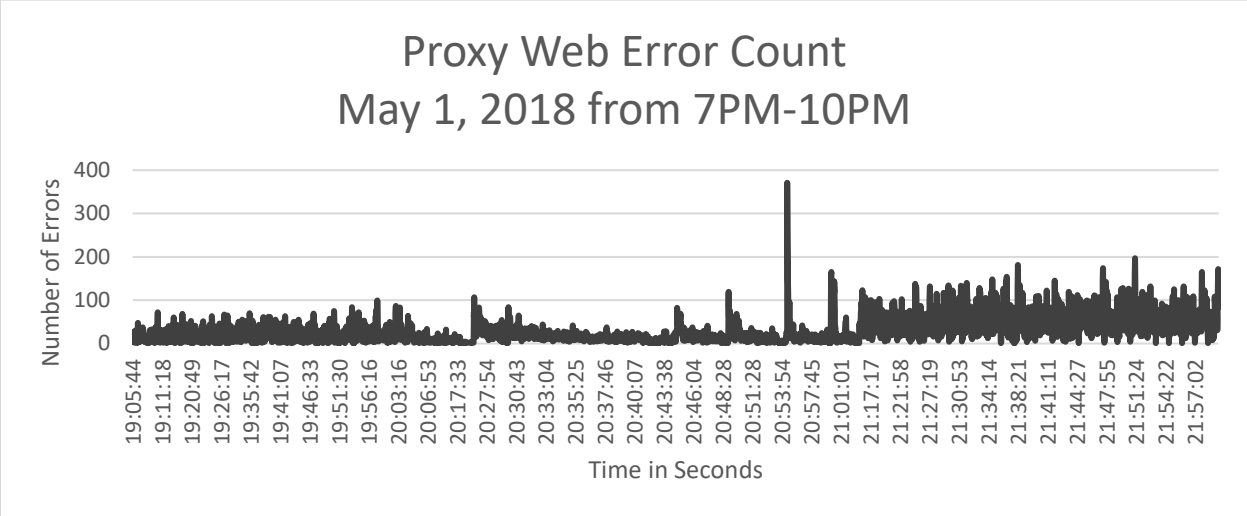
- There was a very large increase in Web server traffic compared to April 30th.
- The number of errors per second on the Proxy server was very high on May 1st compared to captured log traffic for different time periods.
- There is evidence of an active attack on the Web server between the hours of 7PM and 10PM unrelated to a typical Denial of Service (DOS) attack.
- In addition to the active attack on the Web server, additional symptoms of a DOS attack occurred between 7PM and 10PM.
- A large number of foreign countries (~65) accessed the Web site between 7PM and 10PM.
- Due to the lack of network connectivity and the fact that all data that goes into the isolated master system can be validated back to each polling station and to each polling machine, no compromise of official election data could have been carried out. Physical access is closely guarded and therefore would continue to be the only way to manipulate official data.

The combination of the increased Web server activity in conjunction with the active attack on the Web server is the most likely reason for the outage of the Web site. While the intention of the attack cannot be definitively known, the overall effect was very similar to a DOS attack.

Findings

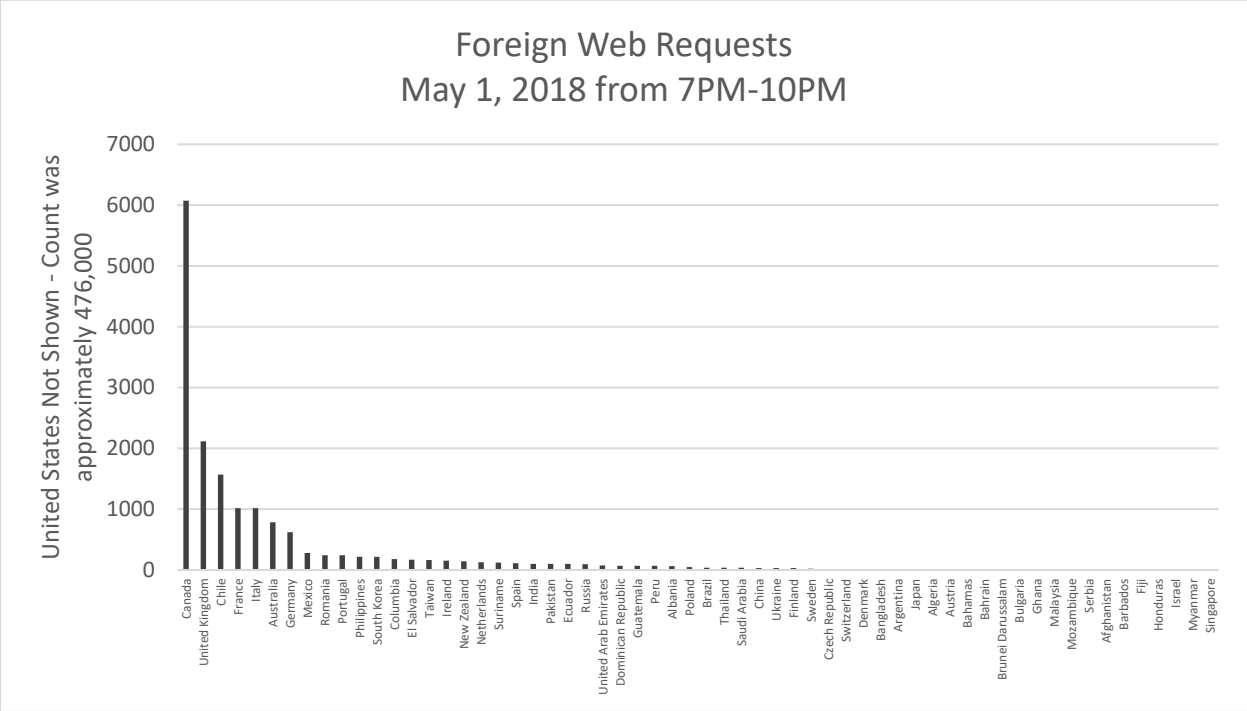
Proxy Web Errors

Sword & Shield focused its primary analysis on the hours between 7PM and 10PM on May 1, 2018. During this time, the Web site saw a large increase in traffic and errors. While some of the error count can be attributed to the Web server being rebooted, the amount of errors is significant. When looking into the errors, Sword & Shield found that most of them were connection errors. These can usually be attributed to a high volume of traffic during which the site cannot keep up with the requests. However, there were numerous specific errors that are of bigger concern. There is evidence of multiple attempts to attack a vulnerability on the Web site itself. The details of this attack can be found later in this report.



Foreign Web Requests

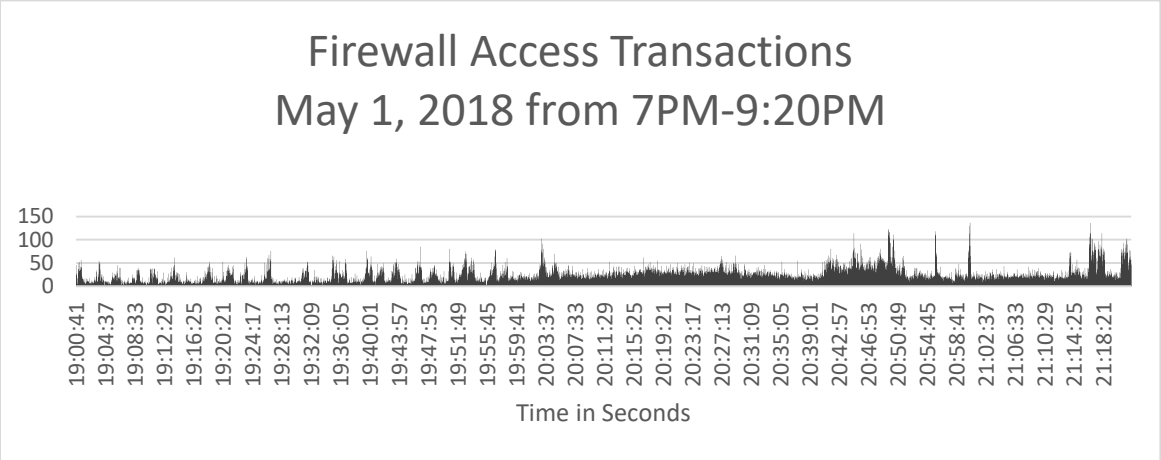
While analyzing the logs, Sword & Shield collected the IP Addresses listed in the logs and parsed them through a geolocation program to determine the country of origin. In addition, Sword & Shield ran calculations of the number of requests from each country between the hours of 7PM and 10PM. There was a suspicious number of unique foreign countries (~65) making requests for such a short amount of time. While the chart below does not expand beyond the 7PM to 10PM time period, Sword & Shield observed an additional 33 countries making requests over the entire day of May 1st totaling close to 100. Below is a chart summary of the occurrences and a table for easier reference to details. More analysis over a longer period of time is needed to determine if the foreign country traffic patterns are normal or anomalous.



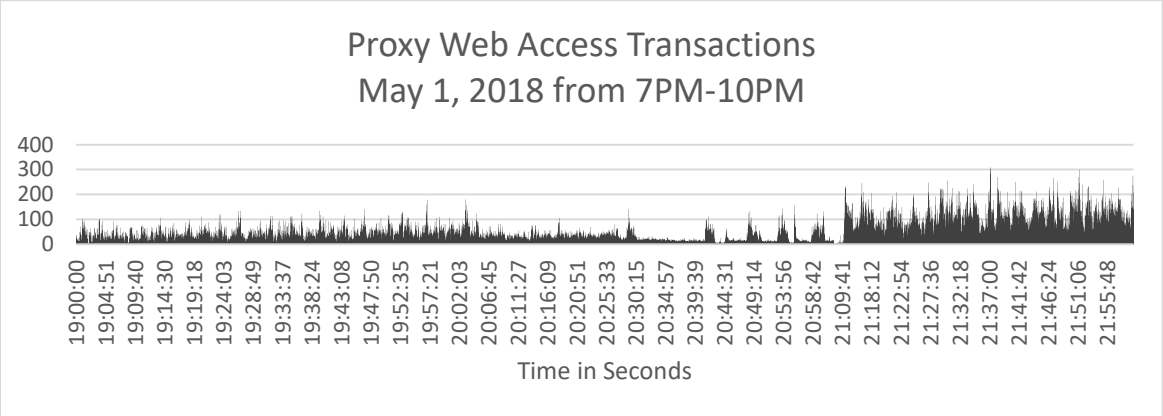
Country	Count		Country	Count
United States	475832		Brazil	39
Canada	6072		Thailand	36
United Kingdom	2116		Saudi Arabia	35
Chile	1571		China	34
France	1018		Ukraine	34
Italy	1016		Finland	33
Australia	787		Sweden	22
Germany	624		Czech Republic	10
Mexico	278		Switzerland	6
Romania	242		Denmark	5
Portugal	240		Bangladesh	4
Philippines	218		Argentina	3
South Korea	218		Japan	3
Columbia	179		Algeria	2
El Salvador	167		Austria	2
Taiwan	164		Bahamas	2
Ireland	151		Bahrain	2
New Zealand	145		Brunei Darussalam	2
Netherlands	128		Bulgaria	2
Suriname	120		Ghana	2
Spain	111		Malaysia	2
India	103		Mozambique	2
Pakistan	101		Serbia	2
Ecuador	98		Afghanistan	1
Russia	95		Barbados	1
United Arab Emirates	75		Fiji	1
Dominican Republic	70		Honduras	1
Guatemala	70		Israel	1
Peru	70		Myanmar	1
Albania	64		Singapore	1
Poland	48			

Traffic Volume

There was a high amount of Web server traffic on May 1st. The evidence of this is shown in the following charts. The first chart shows individual firewall transactions specifically between 7PM-9:20PM. Sword & Shield did not analyze log data beyond 9:20PM since that is when the supplied log data stopped.



Between 7PM and 10PM, the Proxy Web server also showed a significantly high amount of traffic. The chart below shows the individual Proxy server transactions during this period.



The traffic details shown from a Google Analytics report gives a picture of just how much the Web traffic increased on May 1st compared to April 30th. Below is a small sample of the information, but it is important to note that the Google Analytics' report does not include numbers for incomplete transactions in the pageview numbers. This sample makes it clear that overall traffic was exponentially higher. The percentage increase is one data point but is often mis-leading due to the low baseline number compared to the delta during the Web server's busiest time. This is not to say that the traffic was not significant. Looking only at the percentage numbers presents a skewed picture of the traffic load.

Page	Country	Pageviews	Unique Pageviews	Avg. Time on Page	Entrances	Bounce Rate	% Exit	Page Value
		515.37% ▲ 58,528 vs 9,511	310.21% ▲ 26,561 vs 6,475	137.53% ▲ 00:02:59 vs 00:01:15	363.75% ▲ 17,168 vs 3,702	0.44% ▼ 49.08% vs 48.87%	24.02% ▼ 29.80% vs 39.23%	0.00% $0.00 vs $0.00
1. /election/live.php	United States							
May 1, 2018 - May 1, 2018		**28,957** (49.48%)	7,954 (29.95%)	00:04:00	5,977 (34.81%)	59.44%	25.03%	$0.00 (0.00%)
Apr 30, 2018 - Apr 30, 2018		**52** (0.55%)	33 (0.51%)	00:03:37	24 (0.65%)	70.83%	50.00%	$0.00 (0.00%)
% Change		**55,586.54%**	**24,003.03%**	**10.66%**	**24,804.17%**	**-16.08%**	**-49.95%**	**0.00%**
2. /election/index.php	United States							
May 1, 2018 - May 1, 2018		**12,922** (22.08%)	8,145 (30.67%)	00:01:23	6,829 (39.78%)	37.19%	33.75%	$0.00 (0.00%)
Apr 30, 2018 - Apr 30, 2018		**3,943** (41.46%)	2,538 (39.20%)	00:01:38	2,270 (61.32%)	47.84%	45.04%	$0.00 (0.00%)
% Change		**227.72%**	**220.92%**	**-15.00%**	**200.84%**	**-22.25%**	**-25.07%**	**0.00%**
3. /election/nav_voter.php	United States							
May 1, 2018 - May 1, 2018		**4,078** (6.97%)	3,037 (11.43%)	00:01:48	992 (5.78%)	60.08%	47.94%	$0.00 (0.00%)
Apr 30, 2018 - Apr 30, 2018		**1,327** (13.95%)	968 (14.95%)	00:01:34	246 (6.65%)	54.47%	42.50%	$0.00 (0.00%)
% Change		**207.31%**	**213.74%**	**15.43%**	**303.25%**	**10.30%**	**12.80%**	**0.00%**
4. /election/results/election_results.php	United States							
May 1, 2018 - May 1, 2018		**3,181** (5.44%)	931 (3.51%)	00:03:58	300 (1.75%)	36.00%	16.57%	$0.00 (0.00%)
Apr 30, 2018 - Apr 30, 2018		**4** (0.04%)	3 (0.05%)	00:01:14	0 (0.00%)	0.00%	50.00%	$0.00 (0.00%)
% Change		**79,425.00%**	**30,933.33%**	**223.94%**	**∞%**	**∞%**	**-66.87%**	**0.00%**
5. /election/upcoming_election.php	United States							
May 1, 2018 - May 1, 2018		**2,009** (3.43%)	1,348 (5.08%)	00:00:24	341 (1.99%)	19.35%	12.49%	$0.00 (0.00%)
Apr 30, 2018 - Apr 30, 2018		**1,209** (12.71%)	798 (12.32%)	00:00:16	216 (5.83%)	11.11%	11.91%	$0.00 (0.00%)
% Change		**66.17%**	**68.92%**	**48.20%**	**57.87%**	**74.19%**	**4.90%**	**0.00%**

Web Site Attack

While analyzing the error logs and traffic logs on the Web server, a number of particularly suspicious events were noted. These events indicated an active attempt to exploit the backend database behind the Web server. While any Web site on the Internet will potentially be probed for vulnerabilities on a routine basis, these attacks indicate that an actual vulnerability exists on the Web server. An additional concern is that the source IPs engaged in the exploit of the vulnerability on the Web server were from non-United states registered IP addresses. One IP was mapped to the Ukraine and the second IP was mapped to Great Britain

Sword & Shield requested permission from Knox County to test the specific exploit that was shown in the logs. Knox County agreed, and Sword & Shield ran through standard scans and tested the specific exploit concurrently. During this time, two key events happened. The first is that Sword & Shield determined that a vulnerability exists that can be exploited. The second is that while performing the test, the Web site crashed. There is not a clear indication whether the Web site crash was due to the traffic of the scan, the vulnerability being accessed, a combination of both or another external factor. Further testing would determine whether the exploit re-creation or the scanning tool traffic resulted in the Web server crash.

Election Results Data Flow

Due to the clear evidence of a successful exploit, Sword & Shield reviewed the architectural design of the Web site, the backend database, flat file storage, and the official election results process with Knox County IT. Knox County explained how the official election results reside in systems that have no network connectivity of any type. Currently, Knox County uses the Hart InterCivic eSlate direct recording electronic voting system. All official voting data collected at each polling station is physically transported to Knox County for consolidation that is observed by election officials. The consolidated election results are stored on an isolated master system. To export the data to the Web site, a memory card is physically carried to a network connected injection station. This process provides data integrity. No data is carried back to the isolated master system that contains the official election results. Due to the lack of network connectivity and the fact that all data that goes into the isolated master system can be validated back to each polling station and to each polling machine, no compromise of official election data could have been carried out. Physical access is closely guarded and therefore would continue to be the only way to manipulate official data.

Denial of Service

A denial of service is defined by the US Department of Homeland Security as follows:

"In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, Web sites, online accounts (banking, etc.), or other services that rely on the affected computer."

Between the hours of 7PM and 10PM on May 1, 2018, the Knox County Web site was in a state that caused users to be unable or barely able to access the site. There was a large number of requests hitting the Web site, a suspiciously large number of foreign countries accessing the Web site, a large number of errors being created and an attack on the Web site all occurring during this period. The Knox County IT Staff had to increase the number of CPUs being used by the Web site from 3 to 16 to overcome the overall event and keep the Web site up. This is certainly typical of the resource changes needed during a typical DOS attack. It is unclear what the specific cause of the outage was due to a multitude of events occurring at the same time. The effect was clearly a loss of service, but it is unclear, with the information provided, if the outage was an intended event or a side effect of the events.

Conclusion

Knox County Tennessee contracted Sword & Shield Enterprise Security Inc. (Sword & Shield) to conduct a Root Cause Analysis. The objective of the analysis was to ascertain the root cause of a Web site outage on May 1, 2018. Logs from the Knox County firewall, Proxy server and Web server were given to Sword & Shield for event correlation and review.

After analyzing the supplied information, Sword & Shield was able to determine that there was a large increase in overall traffic, a suspiciously large number of foreign countries accessing the Web site, a large number of errors were recorded in the logs, and a specific attack on a Web site vulnerability was being performed. Some or all of these factors are the likely cause of the outage.