JANUARY 2017 Volume 6 Issue 1

# VE3ERC-LUB

ELMIRA RADIO CLUB
VE3 ERC

**President: Joycee VA3WXU**
**Vice-President: John VE3JXX**
**Secretary: Tom VE3DXQ**
**Treasurer: Reg VE3RVH**
**Trustee: Al VA3TET**
**QSL Manager: Judd VE3WXU**
**Repeater Manager & Maintenance: Carl VE3FEF**
**Website Admin: Ted VE3TRQ**
**Lighthouse: Bruce VE3QB**
**Maple Syrup Display: Judd VE3WXU**
**Joycee VA3WXU**
**Newsletter: Bob VE3IXX**

## ERC REPEATERS

**UHF 444.700 TONE: 131.8**
**VHF 147.390 + TONE: 123.0**
**EMERGENCY SIMPLEX: 147.51**

**Emergency Reminder:**
**In the event of an emergency, tune into our repeaters,**
**UHF 444.700 or**
**VHF 147.390 or**
**HF 3.755 LSB or**
**Simplex 147.510**
**For coordination and assignments.**

Radio Amateurs of Canada


VE3CRU Bill's Rover Van at the York Region Hamfest.

# THE PREZ SEZ!

## This club is Radio-ACTIVE

### President's Update for January 2017

## A New View..... A New Year

Welcome back everyone! The holidays overly granted us our traditional wish for a white Christmas. I hope that the holidays were as generous in bringing you health, joy, laughter, and something you could use in your shack!

At our last meeting in November, we were working on several different club matters that need to be revisited in the new year. This includes the following:

-Rich (VE3DCC) had had a meeting with Ron Koniuch from CARE and Kieran and Kelly from the fire department. These people confirmed we are in the emergency plan. It was suggested that the next step would be to get ARES training.

-Jim (VE3JMU) and John (VE3JXX) took down the antenna and mast at the feed mill partially because the roof was being stripped off and replaced.

-Al (VA3TET) advised that he had been under the weather and was not able to get to the sale of Bill Graham's equipment as he earlier wanted.

-Joycee (VA3WXU) put forth a suggestion to raise money for the club to cover the insurance deductible. Tail gating and selling a club radio were suggestions to raise some money.

-Judd (VE3WXU) Gave a handout on Digital basics for beginners on operating in digital mode and set up a training net.

-Ted (VE3TRQ) did a demonstration of FLDIGI and other digital modes. He informed everyone what equipment would be needed.

- In December, Al (VA3TET) was a busy beaver working on at least two antennas and maybe more than that, which will be going up either at the firehall, the mill feed, or at the Maple Syrup Festival.
-

-Several members recently purchased DMRs and are presently learning the "ins and outs" of these radios. Hopefully someone will present the skinny on them at a meeting soon.

Based on the above, there are a few things that we may want to get better organized this year. For example, we should firm up our emergency committee. An updated current roster of the committee is wanting, as well as, a list of the kind of equipment we have and its location. We should take some time to practice our emergency plan at least two or three times a year. Finally, training in ARES and in a variety of digital modes is a good place to start.

The Maple Syrup Festival is coming up fast. One of the things that we need to do this year is to establish a schedule of who would be manning a station so that we are never off the air. We also need to fix the club's Icom 746 **soon** so that we have two working HF rigs there.

**73 Cheers Joycee (VA3WXU)**

---

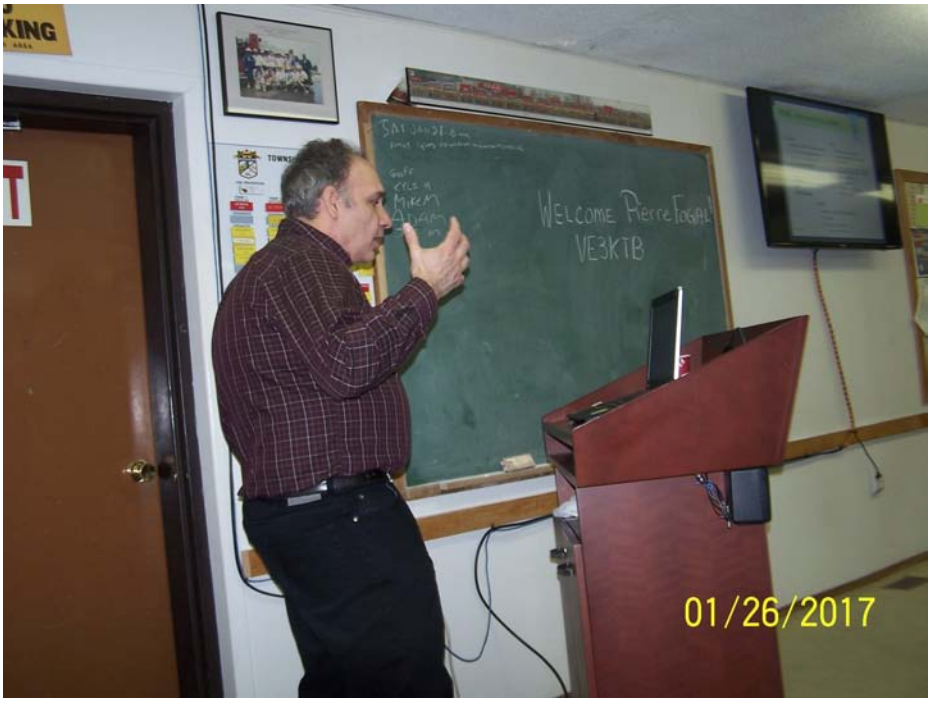
# A Special Ham - VE3KTB

**By Joycee Hodge VA3WXU**

Over a year ago, Tracey Goulding told me that she had seen a wonderful presentation by a Ham, Pierre Fogal (VE3KTB), that works in the Arctic. She highly recommended that I should try to get him to come to Elmira and do a presentation for us.

I kept that thought in my mind for many months when out of the blue, on December 19th, I finally got my chance to meet him. It was Tracey who pointed him out to me in the crowd. Wasting no time, I marched right over to him and held out my hand and introduced who I was and what I wanted. At first, I was met with silence and a solemn, shocked face that quickly transformed into a smile. "Yes," he said, "I will do it." It was very clear to me that Pierre is not afraid to take a risk....


Joycee VA3WXU with Pierre




We were very fortunate that Pierre came to our meeting. The information



Ken VE3KCY with Pierre.

he shared with us was eye-opening. The Arctic is not just a cold, bleak, empty place. The "snow-scapes", "ice-scapes", and "sky-scapes" are all beautiful. It is a land that is habited by an array of interesting animals that seem to thrive there. The cold weather and the environment can be challenging in many ways, including on ham operation, but to those who take risks, it is still worth the trip.

Our club members came out in force to the meeting. Their high expectations of what they were going to learn were reached through the abundance of the questions that were asked and answered. It was very inspiring to look into the Canadian Arctic through the eyes of another Ham who also works under a club call sign that ends in ERC.



A full house came out to hear Pierre's presentation.

# VE3ERC Elmira Radio Club Inc.

***Minutes from Jan 25, 2017***

1. Open and roll call.

The meeting was opened by our President VA3WXU Joycee at 7:30 pm.

Joyce passed around a thank you card from Marie for inviting her to our Christmas party. Marie was wife to VE3ETK Bill. (Silent key)

**Roll Call**: VA3TET Al, VE3DXQ Tom, VE3WXU Jud, VA3WXU Joyce, VE3DCC Rich, VE3QB Bruce, VA3DXK Brian, VA3FJM Frank, VE3TRQ Ted, VE3EIX Harry, VA3GWM Gord, VE3CXU Doug, VE3JMU Jim, VE3KCY Ken, VA3SQD Dan, VE3AHP Rob, VE3EIX Harry, VE3JXX John, VA3KXX Kathy, Johan VA3JVO, Andy VE3CDF, Rich VE3DCC, VE3GSM Greg,VE3PDC Paul, VE3DC Harold, VE3LGN Larry,VE3JVG Jason, Dave (Guest), VE3KTB Pierre.

**Speakers/Program/ Discussions**

Introduction to Pierre Fogal VE3KTB: Joyce VA3WXU mentioned she only met Pierre in December and asked if he could put on a presentation for our club and he said yes. Joyce VA3WXU said it was very kind of him to do so.

Pierre's presentation: Pierre thanked Joycee for her kind introduction. He works for the University of Toronto as the PEARL (Polar Environment Atmospheric Research Laboratory), site manager. The facility is located at Nunavut Ellesmere Island at 15 km from Eureka, a remote weather station, and about 1,100 km from the North Pole. The geographical location is: 80°N, 86°25'W. PEARL monitors the atmosphere.

Pierre said he recently got his Canadian amateur License in January 2014. Before that he had his American License in 2000 as KC0IGY at Denver Colorado. Pierre is originally from Guelph Ontario.

PEARL is part of CANDAC-(Canadian Network for Detection of Atmospheric Change). There are 3 Labs; Ridge, Opal, and Safire. See link http://www.candac.ca/candac/Facilities/kmz.php.

Pierre spoke about the construction and layout of the facilities. He also advised they measure, temperature, pressure, wind speed, light, decay of meteor trails, particles, precipitation, Global Radiation. The site is manned 320 days per year.

The Anik-D satellite is used for communication. This is very expensive. So it is used sparingly to get data to the public.

Pierre advised that the polar- regions are very important to global circulation. Therefore it is important for global climate. Pierre also explained why ground base measurements are important as a means of verifying satellite measurements. The staff are working on a 3 month rotation basis. Power is provided by Diesel and water by snow melt.

Pierre advised that prior to satellite communications HF was the way to communicate. The Amateur radio club at the Ridge Lab is VY0ERC. Pierre showed the various antennas used. Some are home brew.

They can't use more than 100 watts power so as not to interfere with instruments. Also there is wild life in the area such as wolves, Musk-Ox, caribou, Arctic Hare, birds, foxes and there are also flowers in the summer. There was a Q&A at the end of Pierre's presentation.


**New Antenna presentation from Ted VE3TRQ:** Ted made a presentation of a home brew log periodic 2M and 70cm antenna. The design came from Al VA3TET who found it on the internet. He made it with 6 pieces of 5ft aluminum tubing and a couple of lengths of ½ " square tubing. He spent a lot of time threading and screwing the aluminum tubing into the square rails. The ratios of how the elements are placed are what makes it work. There were 18 tubes in total. There are 2 booms or rails on it and the ground of the coax is attached to one rail and centre conductor attached to the other rail. It is supported at the end. The instructions for this antenna are on the VE3ERC website.

**Reports and Announcements: Executive, Committee Chairs, and Members:** Minutes from November meeting. Tom VE3DXQ made a motion to have November minutes accepted. That was seconded by Brian VA3DXK.

Treasurer's Report: Reg VE3RVH was not present, however AL VA3TET gave the report for Reg. Al gave us the current balance. He also advised that monies were sent to the RAC insurance people. We have been insured by RAC since Jan 1, 2017.

Safety Officer Committee: Tom VE3DXQ. Joycee VA3WXU asked Tom about the Safety vests and cones and their whereabouts. Tom advised he has six small cones and AL VA3TET has 10 vests. Al advised he will get the vests over to Tom.

Antenna Committee and Emergency committee: Joycee VA3WXU asked those present if we need these 2 items at every meeting. Rich VE3DCC advised that it is probably a good Idea just so something does not get left on the back burner.

Elmira Maple Syrup Festival: Judd VE3WXU said the application and fees have been sent in. We will have 2 tables, the same as last year. Judd passed around a volunteer signup sheet. He advised that it will be good to know who will be there and what equipment they will operate well ahead of time. He also said that Saturday morning we will be operating ONTARS, probably starting with Bob VE3IXX. Al VA3TET advised we will be also using an 80M PV antenna on ONTARS.

Joycee VA3WXU advised she has been trying to get us in the little book that comes out with the Record and the Observer regarding the maple syrup festival, but keeps getting the run around.

QSL Manager: Judd VE3WXU advised all QSLs were up to date.

Light house report: AL VA3TET nothing to report at this time.

Website Manager: Ted VE3TRQ- Joycee VA3WXU advised that Ted has done a lot of work lately with the website, and Joycee advised that she is very happy with it. Ted advised that there is still more updates coming.


**Unfinished Business:** Ares Training. This is from the November minutes. Rich VE3DCC advised in the November minutes that we need to get ARES training. Rich advised that at the last Emergency committee meeting he gave Joycee VA3WXU a USB with the ARES training manual on it. Rich also advised we should have a few people from the club go through the training and get accredited. This can also be done on line. Joycee asked that those that are interested in ARES training email her and let her know.

Antennas at the feed mill: Al VA3TET talked about the possibilities of expanding our 2m coverage by having the antenna up at the feed mill. To do that we are going to need a new container to accommodate a VHF and UHF repeater. Also we would like to have the 2M repeater connected to the internet. This could be done with a mesh network or a link to a radio where there is an internet connection. The mesh network would be a fixed connection, as opposed to a radio link with a PC/internet connection that could be moved more easily.

Another consideration is, do we want to use IRLP, Echo-link, or All-star.

John VE3JXX agreed that it will be great to have both 440 and 2M at the feed mill for better coverage. He also advised that where the equipment presently is, it is very hard to get to. So he has suggested that a new box of a bigger size would not fit on the cat walk where it is. He is suggesting we have the equipment at ground level for 24hr and easy access. Also to keep the antenna where it is and run the coax to ground level where the repeaters could be. John VE3JXX advised to get a different Antenna also as diamonds do not hold up very well under adverse weather conditions. There will have to be an electrical outlet also. There could also be battery backup for the repeaters.

John VE3JXX's contact at the Arena says a repeater there is still a possibility. This should be pursued sooner rather than later as his contact will retire in a couple of years. John also mentioned that Woolwich Township approved $46,000.00 in grants. John advised that we should apply for a grant as part as emergency services. John volunteered Rich VE3DCC to look into this and also help with it. John also mentioned that the maple syrup festival also gives out grants, but smaller amounts.

Meeting closed at 9:15 pm

## WEDNESDAY NITE NET CONTROLLERS

JANUARY 11 - AL VA3TET
JANUARY 18 - REG VE3RVH
JANUARY 25 - M E E T I N G
FEBRUARY 1 - TOM VE3DXQ
FEBRUARY 8 - PAUL VE3PVB
FEBRUARY 15 - TRACY (VE3JVG)
FEBRUARY 22 - M E E T I N G
MARCH 1 - BRIAN VA3DXK
MARCH 8 - BOB VE3IXX
MARCH 15 - JUDD VE3WXU
MARCH 22 - M E E T I N G
MARCH 29 - TED VE3TRQ + DIGITAL GROUP


CHRISTMAS 365 DAYS A YEAR
STEALTH ANTENNA

# Back-of-the-Napkin Eyeball

## QSO notes and stuff

### by Rich, ve3DCC

**Here are two startling and upsetting thoughts:**

**First**, recently 35 Russian diplomats were expelled from the USA for interfering with the American election. The Dec. 29, 2016 report by US Department of Homeland Security that initiated that action is attached. Note that the header indicates that the document may be distributed without restriction.

**Second**, at a recent KWARC meeting, a representative from the RCMP presented information on how to protect your passwords and computer networks.

**Here is how this is a concern for us.**

As communications enthusiasts, we are directly affected by cyber-interference. Our experiments with transmission of emergency data down a MESH or digi "spine" can be compromised. We are an "open" and "plain-text" based hobby. Our transmissions cannot be coded or encrypted. Despite this, on certain frequencies, you can still copy code groups of 5 characters that have no particular coherence. It is anyone's guess what the intended purpose is. The point here is that there are those out there who do not play by "the rules", and perhaps mean us harm.

The Grizzly-Steppe activity is of particular concern because it used techniques that are readily accessible to hackers of any age and nationality. The code that is included on page 5 is typical of the kind of internal grenade that can be embedded into an unsuspecting machine. No doubt, there is far more revealing code that has not been released. In the January 6, White House briefing, a detailed report was released with the suggestion that the order to embarrass the USA originated with Russian President Putin. The document purposely did not provide details so as to not compromise channels. After the briefing, President-elect Trump stated that his election was not influenced. As of today, those spear-phishing activities are ongoing.

So what is one to do or think?

Page 5 of the attached December report contains a list of actions one should take to protect networks. There is a strong suggestion that logs for IP addresses be examined.

Page 6 outlines a variety of means used to attack systems: Injection Flaws, Cross-site scripting and known server vulnerabilities. Sadly, the internet is replete with information that supports these destructive incursions. The attacks take advantage of our tendency to naively trust machines and the services and information they deliver to us so BEWARE-NOT SO!

You need to look at the list of recommended mitigations on pages 6 to 12, and, perhaps, it is appropriate to ask which of these we may want to include in our own implementations and operating procedures as we start to develop our own emergency digi-networks. We have always assumed that our radio communications had to be both flexible (ad-hoc) and robust enough to survive "natural" disasters. Could we survive a planned and intentional disaster?

We enjoy the privileges of our licenses predicated on our responsibility and expertise. How do we ensure that we reciprocate the trust put in our "ad-hoc" skills.

**De Rich, ve3DCC**

**Attached: JAR-16-20296 (a Joint Analysis Report from Homeland Security, NCCIC,FBI)**

NCCIC

Federal Bureau of Investigation

Federal Bureau of Investigation

***DISCLAIMER:*** *This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as* ***TLP:WHITE:*** *Subject to standard copyright rules,* ***TLP:WHITE*** *information may be distributed without restriction. For more information on the Traffic Light Protocol, see h*[*ttps://www.us-cert.gov/tlp*](https://www.us-cert.gov/tlp)

**Reference Number: JAR-16-20296** **December 29, 2016**

# GRIZZLY STEPPE – Russian Malicious Cyber Activity

## Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities. This determination expands upon the Joint Statement released October 7, 2016, from the Department of Homeland Security and the Director of National Intelligence on Election Security.

This activity by RIS is part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information. In foreign countries, RIS actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. This JAR provides technical indicators related to many of these operations, recommended mitigations, suggested actions to take in response to the indicators provided, and information on how to
report such incidents to the U.S. Government.

## Description

The U.S. Government confirms that two different RIS actors participated in the intrusion into a U.S. political party. The first actor group, known as Advanced Persistent Threat (APT) 29, entered into the party's systems in summer 2015, while the second, known as APT28, entered in spring 2016.

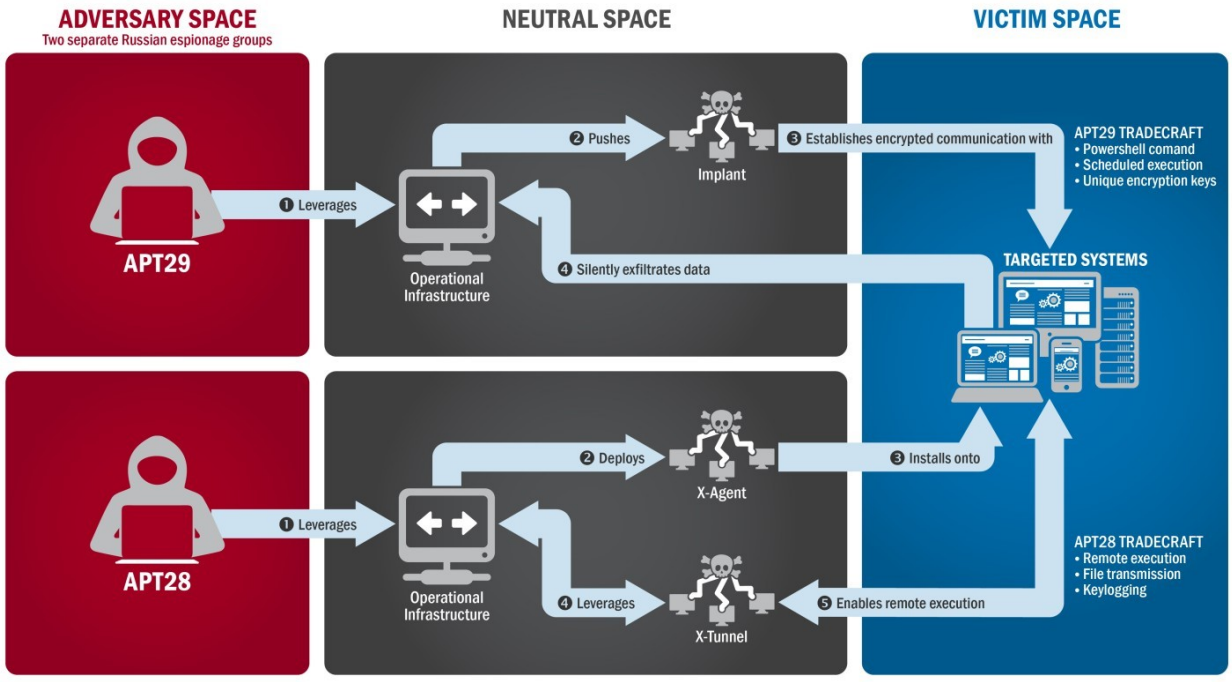



**Figure 1: The tactics and techniques used by APT29 and APT 28 to conduct cyber intrusions against target systems**

Both groups have historically targeted government organizations, think tanks, universities, and corporations around the world. APT29 has been observed crafting targeted spearphishing campaigns leveraging web links to a malicious dropper; once executed, the code delivers Remote Access Tools (RATs) and evades detection using a range of techniques. APT28 is known for leveraging domains that closely mimic those of targeted organizations and tricking potential victims into entering legitimate credentials. APT28

actors relied heavily on shortened URLs in their spearphishing email campaigns. Once APT28 and APT29 have access to victims, both groups exfiltrate and analyze information to gain intelligence value. These groups use this information to craft highly targeted spearphishing campaigns. These actors set up operational infrastructure to obfuscate their source infrastructure, host domains and malware for targeting organizations, establish command and control nodes, and harvest credentials and other valuable information from their targets.

In summer 2015, an APT29 spearphishing campaign directed emails containing a malicious link to over 1,000 recipients, including multiple U.S. Government victims. APT29 used legitimate domains, to include domains associated with U.S. organizations and educational institutions, to host malware and send spearphishing emails. In the course of that campaign, APT29 successfully compromised a U.S. political party. At least one targeted individual activated links to malware hosted on operational infrastructure of opened attachments containing malware. APT29
delivered malware to the political party's systems, established persistence, escalated privileges, enumerated active directory accounts, and exfiltrated email from several accounts through encrypted connections back through operational infrastructure.

In spring 2016, APT28 compromised the same political party, again via targeted spearphishing. This time, the spearphishing email tricked recipients into changing their passwords through a fake webmail domain hosted on APT28 operational infrastructure. Using the harvested credentials, APT28 was able to gain access and steal content, likely leading to the exfiltration of
information from multiple senior party members. The U.S. Government assesses that information was leaked to the press and publicly disclosed.

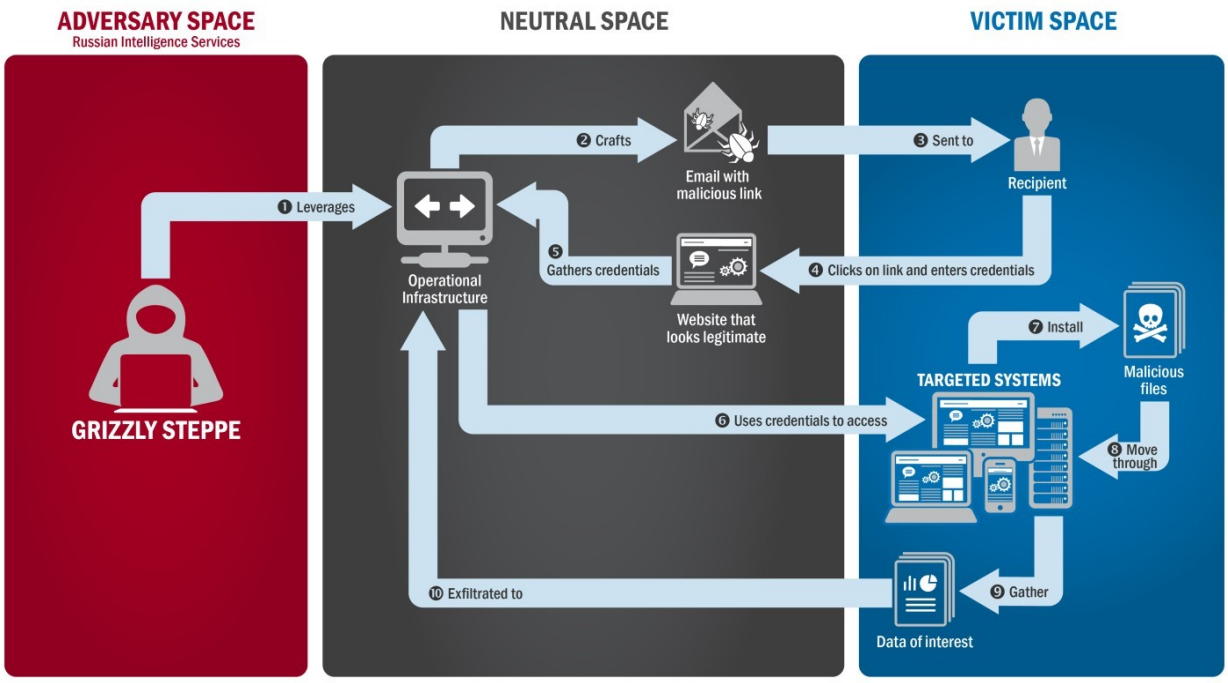



**Figure 2: APT28's Use of Spearphishing and Stolen Credentials**

Actors likely associated with RIS are continuing to engage in spearphishing campaigns, including one launched as recently as November 2016, just days after the U.S. election.

## *Reported Russian Military and Civilian Intelligence Services (RIS)*

| |
|---|
| APT28 |
| APT29 |
| Agent.btz |
| BlackEnergy V3 |
| BlackEnergy2 APT |
| CakeDuke |
| Carberp |
| CHOPSTICK |
| CloudDuke |
| CORESHELL |
| CosmicDuke |
| COZYBEAR |
| COZYCAR |
| COZYDUKE |
| CrouchingYeti |
| DIONIS |
| Dragonfly |
| Energetic Bear |
| EVILTOSS |
| Fancy Bear |
| GeminiDuke |
| GREY CLOUD |
| HammerDuke |
| HAMMERTOSS |
| Havex |
| MiniDionis |
| MiniDuke |
| OLDBAIT |
| OnionDuke |
| Operation Pawn Storm |
| PinchDuke |
| Powershell backdoor |
| Quedagh |
| Sandworm |
| SEADADDY |
| Seaduke |
| SEDKIT |
| SEDNIT |
| Skipper |
| Sofacy |
| SOURFACE |
| SYNful Knock |
| Tiny Baron |
| Tsar Team |
| twain_64.dll (64-bit X-Agent implant) |
| VmUpgradeHelper.exe (X-Tunnel implant) |
| Waterbug |
| X-Agent |

## Technical Details

### *Indicators of Compromise (IOCs)*

IOCs associated with RIS cyber actors are provided within the accompanying .csv and .stix files of JAR-16-20296.

### *Yara Signature*

```
rule PAS_TOOL_PHP_WEB_KIT
{
meta:
description = "PAS TOOL PHP WEB KIT FOUND"
strings:
$php = "<?php"
$base64decode = /\='base'\.\(\d+\*\d+\)\.'_de'\.'code'/
$strreplace = "(str_replace("
$md5 = ".substr(md5(strrev("
$gzinflate = "gzinflate"
$cookie = "_COOKIE"
$isset = "isset" con-
dition:
(filesize > 20KB and filesize < 22KB) and
#cookie == 2 and
#isset == 3 and all of
them
}
```

### *Actions to Take Using Indicators*

DHS recommends that network administrators review the IP addresses, file hashes, and Yara signature provided and add the IPs to their watchlist to determine whether malicious activity has been observed within their organizations. The review of network perimeter netflow or firewall logs will assist in determining whether your network has experienced suspicious activity.

When reviewing network perimeter logs for the IP addresses, organizations may find numerous instances of these IPs attempting to connect to their systems. Upon reviewing the traffic from these IPs, some traffic may correspond to malicious activity, and some may correspond to legitimate activity. Some traffic that may appear legitimate is actually malicious, such as vulnerability scanning or browsing of legitimate public facing services (e.g., HTTP, HTTPS, FTP). Connections from these IPs may be performing vulnerability scans attempting to identify websites that are vulnerable to cross-site scripting (XSS) or Structured Query Language (SQL) injection attacks. If scanning identified vulnerable sites, attempts to exploit the vulnerabilities may be experienced.

Network administrators are encouraged to check their public-facing websites for the malicious file hashes. System owners are also advised to run the Yara signature on any system that is suspected to have been targeted by RIS actors.

### *Threats from IOCs*

Malicious actors may use a variety of methods to interfere with information systems. Some methods of attack are listed below. Guidance provided is applicable to many other computer networks.

- ***Injection Flaws*** are broad web application attack techniques that attempt to send commands to a browser, database, or other system, allowing a regular user to control behavior. The most common example is SQL injection, which subverts the relationship between a webpage and its supporting database, typically to obtain information contained inside the database. Another form is command injection, where an untrusted user is able to send commands to operating systems supporting a web application or database. See the United States Computer Emergency Readiness Team (US-CERT) Publication on SQL Injection for more information.
- ***Cross-site scripting (XSS) vulnerabilities*** allow threat actors to insert and execute unauthorized code in web applications. Successful XSS attacks on websites can provide the attacker unauthorized access. For prevention and mitigation strategies against XSS, see US-CERT's Alert on Compromised Web Servers and Web Shells.
- ***Server vulnerabilities*** may be exploited to allow unauthorized access to sensitive information. An attack against a poorly configured server may allow an adversary access to critical information including any websites or databases hosted on the server. See US-CERT's Tip on Website Security for additional information.

## Recommended Mitigations

### *Commit to Cybersecurity Best Practices*

A commitment to good cybersecurity and best practices is critical to protecting networks and systems. Here are some questions you may want to ask your organization to help prevent and mitigate against attacks.

1. **Backups**: Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis**: Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training**: Have we trained staff on cybersecurity best practices?
4. **Vulnerability Scanning & Patching**: Have we implemented regular scans of our network and systems and appropriate patching of known system vulnerabilities?
5. **Application Whitelisting**: Do we allow only approved programs to run on our networks?
6. **Incident Response**: Do we have an incident response plan and have we practiced it?
7. **Business Continuity**: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing**: Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

### *Top Seven Mitigation Strategies*

DHS encourages network administrators to implement the recommendations below, which can prevent as many as 85 percent of targeted cyber-attacks. These strategies are common sense to many, but DHS continues to see intrusions because organizations fail to use these basic measures.

1. **Patch applications and operating systems –** Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker. Use best practices when updating software and patches by only downloading updates from authenticated vendor sites.
2. **Application whitelisting –** Whitelisting is one of the best security strategies because it allows only specified programs to run while blocking all others, including malicious software.
3. **Restrict administrative privileges –** Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Reduce privileges to only those needed for a user's duties. Separate administrators into privilege tiers with limited access to other tiers.
4. **Network Segmentation and Segregation into Security Zones** – Segment networks into logical enclaves and restrict host-to-host communications paths. This helps protect sensitive information and critical services and limits damage from network perimeter breaches.
5. **Input validation –** Input validation is a method of sanitizing untrusted user input provided by users of a web application, and may prevent many types of web application security flaws, such as SQLi, XSS, and command injection.
6. **File Reputation** – Tune Anti-Virus file reputation systems to the most aggressive setting possible; some products can limit execution to only the highest reputation files, stopping a wide range of untrustworthy code from gaining control.
7. **Understanding firewalls –** When anyone or anything can access your network at any time, your network is more susceptible to being attacked. Firewalls can be configured to block data from certain locations (IP whitelisting) or applications while allowing relevant and necessary data through.

### *Responding to Unauthorized Access to Networks*

**Implement your security incident response and business continuity plan**. It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. Meanwhile, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

**Contact DHS or law enforcement immediately**. We encourage you to contact DHS NCCIC (NCCICCustomerService@hq.dhs.gov or 888-282-0870), the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937) to report an intrusion and to request incident response resources or technical assistance.

## Detailed Mitigation Strategies

### *Protect Against SQL Injection and Other Attacks on Web Services*

Routinely evaluate known and published vulnerabilities, perform software updates and technology refreshes periodically, and audit external-facing systems for known Web application vulnerabilities. Take steps to harden both Web applications and the servers hosting them to reduce the risk of network intrusion via this vector.[1]

- Use and configure available firewalls to block attacks.
- Take steps to further secure Windows systems such as installing and configuring Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and Microsoft AppLocker.
- Monitor and remove any unauthorized code present in any www directories.
- Disable, discontinue, or disallow the use of Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) and response to these protocols as much as possible.
- Remove non-required HTTP verbs from Web servers as typical Web servers and applications only require GET, POST, and HEAD.
- Where possible, minimize server fingerprinting by configuring Web servers to avoid responding with banners identifying the server software and version number.
- Secure both the operating system and the application.
- Update and patch production servers regularly.
- Disable potentially harmful SQL-stored procedure calls.
- Sanitize and validate input to ensure that it is properly typed and does not contain escaped code.
- Consider using type-safe stored procedures and prepared statements.
- Perform regular audits of transaction logs for suspicious activity.
- Perform penetration testing against Web services.
- Ensure error messages are generic and do not expose too much information.

---

[1] http://msdn.microsoft.com/en-us/library/ff648653.aspx. Web site last accessed April 11, 2016.

### *Phishing and Spearphishing*

- Implement a Sender Policy Framework (SPF) record for your organization's Domain Name System (DNS) zone file to minimize risks relating to the receipt of spoofed messages.
- Educate users to be suspicious of unsolicited phone calls, social media interactions, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in social media or email, and do not respond to solicitations for this information. This includes following links sent in email.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL often includes a variation in spelling or a different domain than the valid website (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- Take advantage of anti-phishing features offered by your email client and web browser.
- Patch all systems for critical vulnerabilities, prioritizing timely patching of software that processes Internet data, such as web browsers, browser plugins, and document readers.

### *Permissions, Privileges, and Access Controls*

- Reduce privileges to only those needed for a user's duties.
- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
- Carefully consider the risks before granting administrative rights to users on their own machines.
- Scrub and verify all administrator accounts regularly.
- Configure Group Policy to restrict all users to only one login session, where possible.
- Enforce secure network authentication where possible.
- Instruct administrators to use non-privileged accounts for standard functions such as Web browsing or checking Web mail.

- Segment networks into logical enclaves and restrict host-to-host communication paths. Containment provided by enclaving also makes incident cleanup significantly less costly.
- Configure firewalls to disallow RDP traffic coming from outside of the network boundary, except for in specific configurations such as when tunneled through a secondary VPN with lower privileges.
- Audit existing firewall rules and close all ports that are not explicitly needed for business. Specifically, carefully consider which ports should be connecting outbound versus inbound.
- Enforce a strict lockout policy for network users and closely monitor logs for failed login activity. This can be indicative of failed intrusion activity.
- If remote access between zones is an unavoidable business need, log and monitor these connections closely.
- In environments with a high risk of interception or intrusion, organizations should consider supplementing password authentication with other forms of authentication such as challenge/response or multifactor authentication using biometric or physical tokens.

### *Credentials*

- Enforce a tiered administrative model with dedicated administrator workstations and separate administrative accounts that are used exclusively for each tier to prevent tools, such as Mimikatz, for credential theft from harvesting domain-level credentials.
- Implement multi-factor authentication (e.g., smart cards) or at minimum ensure users choose complex passwords that change regularly.
- Be aware that some services (e.g., FTP, telnet, and .rlogin) transmit user credentials in clear text. Minimize the use of these services where possible or consider more secure alternatives.
- Properly secure password files by making hashed passwords more difficult to acquire. Password hashes can be cracked within seconds using freely available tools. Consider restricting access to sensitive password hashes by using a shadow password file or equivalent on UNIX systems.
- Replace or modify services so that all user credentials are passed through an encrypted channel.
- Avoid password policies that reduce the overall strength of credentials. Policies to avoid include lack of password expiration date, lack of lockout policy, low or disabled password complexity requirements, and password history set to zero.
- Ensure that users are not re-using passwords between zones by setting policies and conducting regular audits.
- Use unique passwords for local accounts for each device.

### *Logging Practices*

- Ensure event logging (applications, events, login activities, security attributes, etc.) is turned on or monitored for identification of security issues.
- Configure network logs to provide enough information to assist in quickly developing an accurate determination of a security incident.
- Upgrade PowerShell to new versions with enhanced logging features and monitor the logs to detect usage of PowerShell commands, which are often malware-related.
- Secure logs, potentially in a centralized location, and protect them from modification.
- Prepare an incident response plan that can be rapidly implemented in case of a cyber intrusion.

### *How to Enhance Your Organization's Cybersecurity Posture*

DHS offers a variety of resources for organizations to help recognize and address their cybersecurity risks. Resources include discussion points, steps to start evaluating a cybersecurity program, and a list of hands-on resources available to organizations. For a list of services, visit https://www.us-cert.gov/ccubedvp. Other resources include:

- **The Cyber Security Advisors (CSA)** program bolsters cybersecurity preparedness, risk mitigation, and incident response capabilities of critical infrastructure entities and more closely aligns them with the Federal Government. CSAs are DHS personnel assigned to districts throughout the country and territories, with at least one advisor in each of the 10 CSA regions, which mirror the Federal Emergency Management Agency regions. For more information, email cyberadvisor@hq.dhs.gov.
- **Cyber Resilience Review (CRR)** is a no-cost, voluntary assessment to evaluate and enhance cybersecurity within critical infrastructure sectors, as well as state, local, tribal, and territorial governments. The goal of the CRR is to develop an understanding and measurement of key cybersecurity capabilities to provide meaningful indicators of an entity's operational resilience and ability to manage cyber risk to critical services during normal operations and times of operational stress and crisis. Visit https://www.cert.org/resilience/rmm.html to learn more about the CERT Resilience Management Model.
- **Enhanced Cybersecurity Services (ECS)** helps critical infrastructure owners and operators protect their systems by sharing sensitive and classified cyber threat information with Commercial Service Providers (CSPs) and Operational Implementers (OIs). CSPs then use the cyber threat information to protect CI customers. OIs use the threat information to protect internal networks. For more information, email ECS_Program@hq.dhs.gov.
- **The Cybersecurity Information Sharing and Collaboration Program (CISCP)** is a voluntary information-sharing and collaboration program between and among critical infrastructure partners and the Federal Government. For more information, email CISCP@us-cert.gov.

- **The Automated Indicator Sharing (AIS)** initiative is a DHS effort to create a system where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat. That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber-attacks. While AIS will not eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks.

  AIS participants connect to a DHS-managed system in the NCCIC that allows bidirectional sharing of cyber threat indicators. A server housed at each participant's location allows each to exchange indicators with the NCCIC. Participants will not only receive DHS-developed indicators, but can share indicators they have observed in their own network defense efforts, which DHS will then share with all AIS participants. For more information, visit https://www.dhs.gov/ais.
- **The Cybersecurity Framework (Framework)**, developed by the National Institute of Standards and Technology (NIST) in collaboration with the public and private sectors, is a tool that can improve the cybersecurity readiness of entities. The Framework enables entities, regardless of size, degree of cyber risk, or cyber sophistication, to apply
  principles and best practices of risk management to improve the security and resiliency of critical infrastructure. The Framework provides standards, guidelines, and practices that are working effectively today. It consists of three parts—the Framework Core, the Framework Profile, and Framework Implementation Tiers—and emphasizes five functions: Identify, Protect, Detect, Respond, and Recover. Use of the Framework is strictly voluntary. For more information, visit https://www.nist.gov/cyberframework or email cyberframework@nist.gov.

## Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat. Include the JAR reference number (JAR-16-20296) in the subject line of all email correspondence. For any questions related to this report, please contact NCCIC or the FBI.

*NCCIC:*
Phone: +1-888-282-0870
Email: NCCICCustomerService@hq.dhs.gov

*FBI:*
Phone: +1-855-292-3937
Email: cywatch@ic.fbi.gov

## Feedback

NCCIC continuously strives to improve its products and services. You can help by answering a few short questions about this product at the following URL:
https://www.us-cert.gov/forms/feedback.