Feb 15 2024

NETMANAGEIT

Intelligence Report

Massive utility scam campaign spreads via online ads

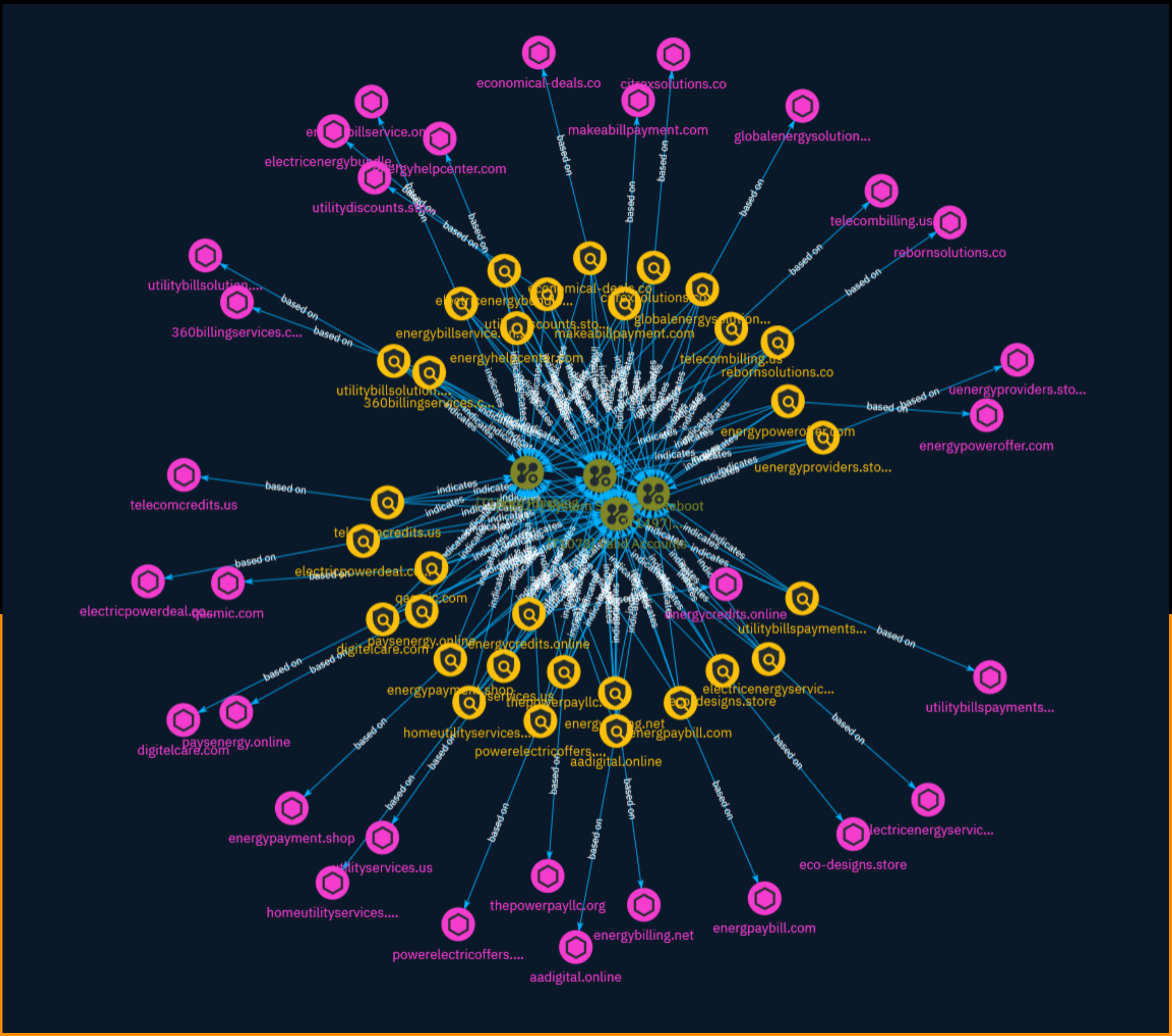

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A recent investigation discovered a prolific campaign of fraudulent ads targeting users searching for keywords related to their energy bills. The ads prompt users to call phone numbers that connect them to utility scammers who threaten and extort money. The scam infrastructure includes dozens of domains and hundreds of ads, mainly targeting US mobile users. This scam is widespread, so avoid clicking any search ads related to utilities and be wary of calls demanding immediate payment.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Indicator

Name
utilityservices.us
Pattern Type
stix
Pattern
[domain-name:value = 'utilityservices.us']
Name
utilitydiscounts.store
Pattern Type
stix
Pattern
[domain-name:value = 'utilitydiscounts.store']
Name
utilitybillspayments.org

Pattern Type

stix

Pattern

[domain-name:value = 'utilitybillspayments.org']

Name

uenergyproviders.store

Pattern Type

stix

Pattern

[domain-name:value = 'uenergyproviders.store']

Name

utilitybillsolution.site

Pattern Type

stix

Pattern

[domain-name:value = 'utilitybillsolution.site']

Name

thepowerpayllc.org

Pattern Type
stix
Pattern
[domain-name:value = 'thepowerpayllc.org']
Name
telecomcredits.us
Pattern Type
stix
Pattern
[domain-name:value = 'telecomcredits.us']
Name
telecombilling.us
Pattern Type
stix
Pattern
[domain-name:value = 'telecombilling.us']
Name
rebornsolutions.co

Pattern Type

stix

Pattern

[domain-name:value = 'rebornsolutions.co']

Name

powerelectricoffers.com

Pattern Type

stix

Pattern

[domain-name:value = 'powerelectricoffers.com']

Name

qasmic.com

Pattern Type

stix

Pattern

[domain-name:value = 'qasmic.com']

Name

paysenergy.online

Pattern Type
stix
Pattern
[domain-name:value = 'paysenergy.online']
Name
makeabillpayment.com
Pattern Type
stix
Pattern
[domain-name:value = 'makeabillpayment.com']
Name
globalenergysolutionz.com
Pattern Type
stix
Pattern
[domain-name:value = 'globalenergysolutionz.com']
Name
homeutilityservices.com

Pattern Type

stix

Pattern

[domain-name:value = 'homeutilityservices.com']

Name

energypoweroffer.com

Pattern Type

stix

Pattern

[domain-name:value = 'energypoweroffer.com']

Name

energypayment.shop

Pattern Type

stix

Pattern

[domain-name:value = 'energypayment.shop']

Name

energyhelpcenter.com

Pattern Type
stix
Pattern
[domain-name:value = 'energyhelpcenter.com']
Name
energycredits.online
Pattern Type
stix
Pattern
[domain-name:value = 'energycredits.online']
Name
energybilling.net
Pattern Type
stix
Pattern
[domain-name:value = 'energybilling.net']
Name
energybillservice.online

Pattern Type

stix

Pattern

[domain-name:value = 'energybillservice.online']

Name

energpaybill.com

Pattern Type

stix

Pattern

[domain-name:value = 'energpaybill.com']

Name

electricpowerdeal.com

Pattern Type

stix

Pattern

[domain-name:value = 'electricpowerdeal.com']

Name

electricenergybundle.com

Pattern Type

stix

Pattern

[domain-name:value = 'electricenergybundle.com']

Name

electricenergyservice.com

Pattern Type

stix

Pattern

[domain-name:value = 'electricenergyservice.com']

Name

economical-deals.co

Pattern Type

stix

Pattern

[domain-name:value = 'economical-deals.co']

Name

eco-designs.store

Pattern Type

stix

Pattern

[domain-name:value = 'eco-designs.store']

Name

digitelcare.com

Pattern Type

stix

Pattern

[domain-name:value = 'digitelcare.com']

Name

citrexsolutions.co

Pattern Type

stix

Pattern

[domain-name:value = 'citrexsolutions.co']

Name

aadigital.online

Pattern Type

stix

Pattern

[domain-name:value = 'aadigital.online']

Name

360billingservices.com

Pattern Type

stix

Pattern

[domain-name:value = '360billingservices.com']

Attack-Pattern

Name
System Shutdown/Reboot
ID
T1529
Description
Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine or network device. In some cases, these commands may also be used to initiate a shutdown/reboot of a remote computer or network device via [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) (e.g. `reload`).(Citation: Microsoft Shutdown Oct 2017)(Citation: alert_TA18_106A) Shutting down or rebooting systems may disrupt access to computer resources for legitimate users while also impeding incident response/recovery. Adversaries may attempt to shutdown/reboot a system after impacting it in other ways, such as [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) or [Inhibit System Recovery](https://attack.mitre.org/techniques/T1490), to hasten the intended effects on system availability.(Citation: Talos Nyetya June 2017)(Citation: Talos Olympic Destroyer 2018)
Name
Valid Accounts
ID

T1078

Description

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Virtualization/Sandbox Evasion

ID

T1497

Description

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness) Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox. (Citation: Unit 42 Pirpi July 2015)

Country

Name
United States

Sector

Name
Energy
Description
Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.

Domain-Name

Value
utilityservices.us
utilitydiscounts.store
utilitybillspayments.org
utilitybillsolution.site
uenergyproviders.store
thepowerpayllc.org
telecomcredits.us
telecombilling.us
qasmic.com
rebornsolutions.co
powerelectricoffers.com
paysenergy.online
makeabillpayment.com

homeutilityservices.com
globalenergysolutionz.com
energypoweroffer.com
energypayment.shop
energyhelpcenter.com
energycredits.online
energybillservice.online
energybilling.net
energpaybill.com
electricpowerdeal.com
electricenergyservice.com
electricenergybundle.com
economical-deals.co
eco-designs.store
digitelcare.com
citrexsolutions.co
aadigital.online
360billingservices.com

External References

- https://www.malwarebytes.com/blog/threat-intelligence/2024/02/massive-utility-scam-campaign-spreads-via-online-ads
- https://otx.alienvault.com/pulse/65ce4709711708cb4a321e2c