**Case Study validation and results focusing on APT42**

This code focuses explicitly on APT42 and related Iranian threat actors, while monitoring for 5G infrastructure vulnerabilities and exploitation patterns. The results follow the conclusion of the Python script.

**Python script:**

from datetime import datetime

import requests

import json

from xml.etree import ElementTree

from typing import Dict, List, Optional

class APT42IntelligenceIntegrator:

    def \_\_init\_\_(self):

        self.sources = {

            'mitre': 'https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json',

            'cisa\_kev': 'https://www.cisa.gov/sites/default/files/feeds/known\_exploited\_vulnerabilities.json',

            'cisa\_alerts': 'https://www.cisa.gov/uscert/ncas/alerts.xml',

            'us\_cert': 'https://www.cisa.gov/uscert/ncas/current-activity.xml',

            'microsoft\_security': 'https://api.msrc.microsoft.com/security-guidance'

        }

        # Expanded APT42 search terms

        self.apt42\_terms = [

            'apt42', 'iran revolutionary guard', 'presidential campaign',

            'election 2024', 'campaign accounts', 'iranian state sponsored',

            'phosphorus', 'charming kitten', 'ta453'  # Known Iranian threat actor aliases

        ]

        # 5G specific terms

        self.five\_g\_terms = [

            '5g', 'network slicing', 'edge computing', 'ran',

            'radio access network', 'core network', 'ultra reliable'

        ]

    def get\_source\_data(self, source\_name: str) -> Optional[Dict]:

        """Enhanced fetch data function with source-specific handling"""

        try:

            print(f"Fetching data from {source\_name}...")

            headers = {'Accept': 'application/json'}

            if source\_name in ['cisa\_alerts', 'us\_cert']:

                headers['Accept'] = 'application/xml'

            response = requests.get(self.sources[source\_name], headers=headers)

            if response.ok:

                if source\_name in ['cisa\_alerts', 'us\_cert']:

                    return self.\_parse\_xml(response.text, source\_name)

                return response.json()

        except Exception as e:

            print(f"Error fetching {source\_name} data: {e}")

        return None

    def \_parse\_xml(self, xml\_content: str, source\_type: str) -> Dict:

        """Parse XML content from different sources"""

        try:

            root = ElementTree.fromstring(xml\_content)

            data = {'entries': []}

            if source\_type == 'cisa\_alerts':

                for item in root.findall('.//item'):

                    entry = {

                        'title': item.find('title').text if item.find('title') is not None else '',

                        'description': item.find('description').text if item.find('description') is not None else '',

                        'date': item.find('pubDate').text if item.find('pubDate') is not None else ''

                    }

                    data['entries'].append(entry)

            elif source\_type == 'us\_cert':

                for item in root.findall('.//entry'):

                    entry = {

                        'title': item.find('title').text if item.find('title') is not None else '',

                        'summary': item.find('summary').text if item.find('summary') is not None else '',

                        'updated': item.find('updated').text if item.find('updated') is not None else ''

                    }

                    data['entries'].append(entry)

            return data

        except Exception as e:

            print(f"Error parsing XML from {source\_type}: {e}")

            return {'entries': []}

    def analyze\_findings(self, source\_data: Dict) -> Dict:

        """Analyze intelligence data for APT42 activities"""

        findings = {

            'campaign\_targeting': [],    # Campaign account compromises

            'disinformation': [],        # Disinformation activities

            '5g\_exploitation': [],       # 5G infrastructure exploitation

            'general\_activities': []     # Other relevant activities

        }

        if 'objects' in source\_data:

            for obj in source\_data['objects']:

                # Check for APT42 related activities

                if any(term in str(obj).lower() for term in self.apt42\_terms):

                    # Categorize by type of activity

                    if any(term in str(obj).lower() for term in ['account', 'credential', 'email']):

                        findings['campaign\_targeting'].append(self.\_format\_finding(obj, 'MITRE', 'campaign\_targeting'))

                    elif any(term in str(obj).lower() for term in ['disinformation', 'propaganda', 'influence']):

                        findings['disinformation'].append(self.\_format\_finding(obj, 'MITRE', 'disinformation'))

                    elif any(term in str(obj).lower() for term in self.five\_g\_terms):

                        findings['5g\_exploitation'].append(self.\_format\_finding(obj, 'MITRE', '5g\_exploitation'))

                    else:

                        findings['general\_activities'].append(self.\_format\_finding(obj, 'MITRE', 'general'))

        return findings

    def \_format\_finding(self, obj: Dict, source: str, category: str) -> Dict:

        """Format finding data consistently"""

        return {

            'source': source,

            'category': category,

            'type': obj.get('type'),

            'name': obj.get('name', 'Unnamed'),

            'description': obj.get('description', 'No description')[:200],

            'timestamp': obj.get('created', 'Date unknown'),

            'risk\_level': self.\_assess\_risk\_level(obj, category)

        }

    def \_assess\_risk\_level(self, obj: Dict, category: str) -> str:

        """Assess risk level based on our ontology's criteria"""

        if category == 'campaign\_targeting' and 'presidential' in str(obj).lower():

            return 'High'

        elif category == '5g\_exploitation':

            return 'High'

        elif category == 'disinformation' and '2024' in str(obj).lower():

            return 'High'

        return 'Medium'

    def correlate\_patterns(self, all\_findings: Dict) -> Dict:

        """Enhanced pattern correlation"""

        correlated\_data = {

            'temporal\_patterns': [],

            'attack\_patterns': [],

            'risk\_distribution': {

                'High': 0,

                'Medium': 0,

                'Low': 0

            },

            '5g\_relevance': {

                'direct': 0,

                'indirect': 0,

                'none': 0

            }

        }

        for category in all\_findings:

            for finding in all\_findings[category]:

                # Count risk levels

                if finding['risk\_level'] in correlated\_data['risk\_distribution']:

                    correlated\_data['risk\_distribution'][finding['risk\_level']] += 1

                # Analyze 5G relevance

                if any(term in finding['description'].lower() for term in self.five\_g\_terms):

                    correlated\_data['5g\_relevance']['direct'] += 1

                elif any(term in finding['description'].lower() for term in ['network', 'infrastructure', 'communication']):

                    correlated\_data['5g\_relevance']['indirect'] += 1

                else:

                    correlated\_data['5g\_relevance']['none'] += 1

                # Add temporal patterns if timestamp exists

                if finding['timestamp'] != 'Date unknown':

                    timestamp = datetime.strptime(finding['timestamp'], '%Y-%m-%dT%H:%M:%S.%fZ')

                    correlated\_data['temporal\_patterns'].append({

                        'date': timestamp,

                        'category': category,

                        'risk\_level': finding['risk\_level']

                    })

        return correlated\_data

    def integrate\_intelligence(self) -> Dict:

        """Main integration function"""

        all\_findings = {}

        for source in self.sources.keys():

            source\_data = self.get\_source\_data(source)

            if source\_data:

                findings = self.analyze\_findings(source\_data)

                for category in findings:

                    if category not in all\_findings:

                        all\_findings[category] = []

                    all\_findings[category].extend(findings[category])

        patterns = self.correlate\_patterns(all\_findings)

        return {

            'findings': all\_findings,

            'patterns': patterns

        }

def main():

    integrator = APT42IntelligenceIntegrator()

    results = integrator.integrate\_intelligence()

    print("\n=== APT42 ANALYSIS RESULTS ===")

    total\_findings = 0

    for category in results['findings']:

        findings\_count = len(results['findings'][category])

        total\_findings += findings\_count

        print(f"\n{category.upper()} FINDINGS")

        print(f"Total findings: {findings\_count}")

        print("=" \* 80)

        for item in results['findings'][category]:

            print(f"\nSource: {item['source']}")

            print(f"Risk Level: {item['risk\_level']}")

            print(f"Type: {item.get('type', 'N/A')}")

            print(f"Name: {item['name']}")

            print(f"Description: {item['description']}")

            print(f"Timestamp: {item['timestamp']}")

            print("-" \* 80)

    print("\n=== RISK DISTRIBUTION ===")

    for risk\_level, count in results['patterns']['risk\_distribution'].items():

        percentage = (count / total\_findings \* 100) if total\_findings > 0 else 0

        print(f"{risk\_level}: {count} findings ({percentage:.1f}%)")

    print("\n=== 5G RELEVANCE ANALYSIS ===")

    total\_5g = sum(results['patterns']['5g\_relevance'].values())

    for relevance\_type, count in results['patterns']['5g\_relevance'].items():

        percentage = (count / total\_5g \* 100) if total\_5g > 0 else 0

        print(f"{relevance\_type.title()}: {count} findings ({percentage:.1f}%)")

if \_\_name\_\_ == "\_\_main\_\_":

    main()

\*\*\*

PS C:\Users\andre> & C:/Users/andre/AppData/Local/Microsoft/WindowsApps/python3.12.exe "c:/Users/andre/ontology/Decoding5G\_test/Documentation for GitHub/2\_intelligence-integration-code\_Jan17.py"

Fetching data from mitre...

Fetching data from cisa\_kev...

Fetching data from cisa\_alerts...

Fetching data from us\_cert...

Fetching data from microsoft\_security...

=== APT42 ANALYSIS RESULTS ===

CAMPAIGN\_TARGETING FINDINGS

Total findings: 18

================================================================================

Source: MITRE

Risk Level: Medium

Type: attack-pattern

Name: Additional Cloud Credentials

Description: Adversaries may add adversary-controlled credentials to a cloud account to maintain persistent access to victim accounts and instances within the environment.

For example, adversaries may add credent

Timestamp: 2020-01-19T16:10:15.008Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: attack-pattern

Name: Multi-Factor Authentication

Description: Adversaries may disable or modify multi-factor authentication (MFA) mechanisms to enable persistent access to compromised accounts.

Once adversaries have gained access to a network by either compromi

Timestamp: 2022-05-31T19:31:38.431Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [ZIRCONIUM](https://attack.mitre.org/groups/G0128) targeted presidential campaign staffers with credential phishing e-mails.(Citation: Google Election Threats October 2020)

Timestamp: 2021-03-25T13:53:09.048Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has established email accounts using fake personas for spearphishing operations.(Citation: IBM ITG18 2020)(Citation: Proofpoint TA453 March 2021)

Timestamp: 2021-03-10T20:32:54.423Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has attempted to lure victims into opening malicious email attachments.(Citation: ClearSky Kittens Back 3 August 2020)

Timestamp: 2021-05-03T19:55:04.095Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has identified high-value email accounts in academia, journalism, NGO's, foreign policy, and national security for targeting.(Citation: Proofpoint

Timestamp: 2021-09-01T20:53:29.877Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has attempted to lure victims into opening malicious links embedded in emails.(Citation: ClearSky Kittens Back 3 August 2020)(Citation: Certfa Char

Timestamp: 2021-05-03T19:55:04.097Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has sent malicious URL links through email to victims. In some cases the URLs were shortened or linked to Word documents with malicious macros that

Timestamp: 2018-04-18T17:59:24.739Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) enabled and used the default system managed account, DefaultAccount, via `"powershell.exe" /c net user DefaultAccount /active:yes` to connect to a

Timestamp: 2023-01-09T19:32:47.671Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used SMS and email messages with links designed to steal credentials or track victims.(Citation: Certfa Charming Kitten January 2021)(Citation:

Timestamp: 2021-05-03T18:58:02.859Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has compromised email credentials in order to steal sensitive data.(Citation: Certfa Charming Kitten January 2021)

Timestamp: 2021-05-03T17:17:12.063Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has stolen domain credentials by dumping LSASS process memory using Task Manager, comsvcs.dll, and from a Microsoft Active Directory Domain Control

Timestamp: 2018-10-17T00:14:20.652Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has exported emails from compromised Exchange servers including through use of the cmdlet `New-MailboxExportRequest.`(Citation: DFIR Report APT35 P

Timestamp: 2022-05-26T14:19:08.287Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used domain administrator accounts after dumping LSASS process memory.(Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-09T20:16:51.095Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has created fake LinkedIn and other social media accounts to contact targets and convince them--through messages and voice communications--to open

Timestamp: 2021-05-03T19:39:06.514Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: intrusion-set

Name: APT28

Description: [APT28](https://attack.mitre.org/groups/G0007) is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) militar

Timestamp: 2017-05-31T21:31:48.664Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: intrusion-set

Name: Magic Hound

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) is an Iranian-sponsored threat group that conducts long term, resource-intensive cyber espionage operations, likely on behalf of the Islamic Revolu

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: intrusion-set

Name: Charming Kitten

Description: [Charming Kitten](https://attack.mitre.org/groups/G0058) is an Iranian cyber espionage group that has been active since approximately 2014. They appear to focus on targeting individuals of interest to

Timestamp: 2018-01-16T00:14:20.562Z

--------------------------------------------------------------------------------

DISINFORMATION FINDINGS

Total findings: 0

================================================================================

5G\_EXPLOITATION FINDINGS

Total findings: 51

================================================================================

Source: MITRE

Risk Level: High

Type: malware

Name: PowerLess

Description: [PowerLess](https://attack.mitre.org/software/S1012) is a PowerShell-based modular backdoor that has been used by [Magic Hound](https://attack.mitre.org/groups/G0059) since at least 2022.(Citation: Cy

Timestamp: 2022-06-01T20:20:02.166Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: tool

Name: FRP

Description: [FRP](https://attack.mitre.org/software/S1144), which stands for Fast Reverse Proxy, is an openly available tool that is capable of exposing a server located behind a firewall or Network Address Trans

Timestamp: 2024-07-10T18:46:33.555Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [PowerLess](https://attack.mitre.org/software/S1012) can use a module to log keystrokes.(Citation: Cybereason PowerLess February 2022)

Timestamp: 2022-06-02T13:17:21.817Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) malware has used Registry Run keys to establish persistence.(Citation: Unit 42 Magic Hound Feb 2017)(Citation: DFIR Phosphorus November 2021)(Citat

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used PowerShell for execution and privilege escalation.(Citation: Unit 42 Magic Hound Feb 2017)(Citation: FireEye APT35 2018)(Citation: DFIR Re

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has obtained and used tools like [Havij](https://attack.mitre.org/software/S0224), [sqlmap](https://attack.mitre.org/software/S0225), Metasploit, [

Timestamp: 2021-05-26T20:14:45.885Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used compromised domains to host links targeted to specific phishing victims.(Citation: ClearSky Kittens Back 3 August 2020)(Citation: Proofpoi

Timestamp: 2021-05-03T19:39:06.488Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used the command-line interface for code execution.(Citation: Unit 42 Magic Hound Feb 2017)(Citation: DFIR Report APT35 ProxyShell March 2022)(

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used Plink to tunnel RDP over SSH.(Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-09T19:38:19.080Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: (Citation: DFIR Report APT35 ProxyShell March 2022)(Citation: DFIR Phosphorus November 2021)

Timestamp: 2022-05-25T19:42:27.787Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: (Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-10T18:57:17.751Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: (Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-05T20:27:17.309Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) malware has used IRC for C2.(Citation: Unit 42 Magic Hound Feb 2017)(Citation: DFIR Phosphorus November 2021)

Timestamp: 2020-03-17T01:49:09.432Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used HTTP for C2.(Citation: Unit 42 Magic Hound Feb 2017)(Citation: DFIR Report APT35 ProxyShell March 2022)(Citation: DFIR Phosphorus November

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used BitLocker and DiskCryptor to encrypt targeted workstations. (Citation: DFIR Phosphorus November 2021)(Citation: Microsoft Iranian Threat A

Timestamp: 2023-01-10T18:36:35.140Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has conducted a network call out to a specific website as part of their initial discovery activity.(Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-03-03T21:56:38.046Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used scheduled tasks to establish persistence and execution.(Citation: DFIR Report APT35 ProxyShell March 2022)(Citation: DFIR Phosphorus Novem

Timestamp: 2022-05-25T18:56:20.248Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used Remote Desktop Services to copy tools on targeted systems.(Citation: DFIR Report APT35 ProxyShell March 2022)(Citation: DFIR Phosphorus No

Timestamp: 2022-06-03T13:31:01.299Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has downloaded additional code and files from servers onto victims.(Citation: Unit 42 Magic Hound Feb 2017)(Citation: DFIR Report APT35 ProxyShell

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [PowerLess](https://attack.mitre.org/software/S1012) has a browser info stealer module that can read Chrome and Edge browser database files.(Citation: Cybereason PowerLess February 2022)

Timestamp: 2022-06-02T13:33:07.971Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [PowerLess](https://attack.mitre.org/software/S1012) can download additional payloads to a compromised host.(Citation: Cybereason PowerLess February 2022)

Timestamp: 2022-06-02T13:15:25.600Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [PowerLess](https://attack.mitre.org/software/S1012) has the ability to exfiltrate data, including Chrome and Edge browser database files, from compromised machines.(Citation: Cybereason PowerLess Feb

Timestamp: 2022-06-02T13:34:56.885Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has exploited the Log4j utility (CVE-2021-44228), on-premises MS Exchange servers via "ProxyShell" (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)

Timestamp: 2022-01-24T16:52:40.660Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used KPortScan 3.0 to perform SMB, RDP, and LDAP scanning.(Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-10T18:25:13.509Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: (Citation: DFIR Phosphorus November 2021)

Timestamp: 2024-07-10T18:54:51.065Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used an encrypted http proxy in C2 communications.(Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-11T18:37:36.996Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: (Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-05T20:28:43.422Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [PowerLess](https://attack.mitre.org/software/S1012) can use an encrypted channel for C2 communications.(Citation: Cybereason PowerLess February 2022)

Timestamp: 2022-06-02T20:02:27.980Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) malware has obtained the victim username and sent it to the C2 server.(Citation: Unit 42 Magic Hound Feb 2017)(Citation: DFIR Report APT35 ProxyShe

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has deleted and overwrote files to cover tracks.(Citation: Unit 42 Magic Hound Feb 2017)(Citation: FireEye APT35 2018)(Citation: DFIR Phosphorus No

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: (Citation: DFIR Report APT35 ProxyShell March 2022)(Citation: DFIR Phosphorus November 2021)

Timestamp: 2022-05-25T19:42:58.107Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [PowerLess](https://attack.mitre.org/software/S1012) can stage stolen browser data in `C:\\Windows\\Temp\\cup.tmp` and keylogger data in `C:\\Windows\\Temp\\Report.06E17A5A-7325-4325-8E5D-E172EBA7FC5B

Timestamp: 2022-06-02T13:37:01.011Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) malware gathers the victim's local IP address, MAC address, and external IP address.(Citation: Unit 42 Magic Hound Feb 2017)(Citation: DFIR Report

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used `dllhost.exe` to mask Fast Reverse Proxy (FRP) and `MicrosoftOutLookUpdater.exe` for Plink.(Citation: DFIR Report APT35 ProxyShell March 2

Timestamp: 2022-05-25T19:40:27.483Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [PowerLess](https://attack.mitre.org/software/S1012) can encrypt browser database files prior to exfiltration.(Citation: Cybereason PowerLess February 2022)

Timestamp: 2022-06-03T13:04:28.122Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has executed scripts to disable the event log service.(Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-11T19:49:30.328Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has copied tools within a compromised network using RDP.(Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-03-03T22:01:18.675Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has added the following rule to a victim's Windows firewall to allow RDP traffic - `"netsh" advfirewall firewall add rule name="Terminal Server" di

Timestamp: 2022-05-26T14:43:14.988Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) malware has communicated with its C2 server over TCP ports 4443 and 10151 using HTTP.(Citation: Unit 42 Magic Hound Feb 2017)(Citation: DFIR Phosph

Timestamp: 2020-03-30T20:57:01.211Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) malware has used a PowerShell command to check the victim system architecture to determine if it is an x64 machine. Other malware has obtained the

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used multiple web shells to gain execution.(Citation: DFIR Report APT35 ProxyShell March 2022)(Citation: DFIR Phosphorus November 2021)

Timestamp: 2022-05-25T18:51:32.312Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [PowerLess](https://attack.mitre.org/software/S1012) is written in and executed via PowerShell without using powershell.exe.(Citation: Cybereason PowerLess February 2022)

Timestamp: 2022-06-02T13:27:48.524Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used Fast Reverse Proxy (FRP) for RDP traffic.(Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-09T20:02:49.885Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has named a malicious script CacheTask.bat to mimic a legitimate task.(Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-10T20:55:51.209Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used [Ping](https://attack.mitre.org/software/S0097) for discovery on targeted networks.(Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-05T20:35:20.182Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: (Citation: Cybereason PowerLess February 2022)

Timestamp: 2022-06-03T12:55:00.108Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used a web shell to execute `nltest /trusted\_domains` to identify trust relationships.(Citation: DFIR Phosphorus November 2021)

Timestamp: 2023-01-11T19:12:58.278Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used gzip to archive dumped LSASS process memory and RAR to stage and compress local folders.(Citation: FireEye APT35 2018)(Citation: DFIR Repo

Timestamp: 2018-10-17T00:14:20.652Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [PowerLess](https://attack.mitre.org/software/S1012) can use base64 and AES ECB decryption prior to execution of downloaded modules.(Citation: Cybereason PowerLess February 2022)

Timestamp: 2022-06-02T13:18:55.848Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has used a web shell to exfiltrate a ZIP file containing a dump of LSASS memory on a compromised machine.(Citation: DFIR Report APT35 ProxyShell Ma

Timestamp: 2022-05-25T19:56:36.080Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: High

Type: intrusion-set

Name: Sandworm Team

Description: [Sandworm Team](https://attack.mitre.org/groups/G0034) is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Tech

Timestamp: 2017-05-31T21:32:04.588Z

--------------------------------------------------------------------------------

GENERAL\_ACTIVITIES FINDINGS

Total findings: 13

================================================================================

Source: MITRE

Risk Level: Medium

Type: malware

Name: DownPaper

Description: [DownPaper](https://attack.mitre.org/software/S0186) is a backdoor Trojan; its main functionality is to download and run second stage malware. (Citation: ClearSky Charming Kitten Dec 2017)

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [DownPaper](https://attack.mitre.org/software/S0186) collects the victim host name and serial number, and then sends the information to the C2 server.(Citation: ClearSky Charming Kitten Dec 2017)

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [DownPaper](https://attack.mitre.org/software/S0186) searches and reads the value of the Windows Update Registry Run key.(Citation: ClearSky Charming Kitten Dec 2017)

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [DownPaper](https://attack.mitre.org/software/S0186) collects the victim username and sends it to the C2 server.(Citation: ClearSky Charming Kitten Dec 2017)

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [DownPaper](https://attack.mitre.org/software/S0186) uses PowerShell to add a Registry Run key in order to establish persistence.(Citation: ClearSky Charming Kitten Dec 2017)

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has registered fraudulent domains such as "mail-newyorker.com" and "news12.com.recover-session-service.site" to target specific victims with phishi

Timestamp: 2021-05-03T19:10:10.755Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: (Citation: ClearSky Charming Kitten Dec 2017)

Timestamp: 2020-05-27T21:22:18.518Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has acquired mobile phone numbers of potential targets, possibly for mobile malware or additional phishing operations.(Citation: Proofpoint TA453 J

Timestamp: 2021-09-01T20:53:29.864Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) used various social media channels (such as LinkedIn) as well as messaging services (such as WhatsApp) to spearphish victims.(Citation: SecureWorks

Timestamp: 2020-07-04T23:30:04.892Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [DownPaper](https://attack.mitre.org/software/S0186) communicates to its C2 server over HTTP.(Citation: ClearSky Charming Kitten Dec 2017)

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [DownPaper](https://attack.mitre.org/software/S0186) uses PowerShell for execution.(Citation: ClearSky Charming Kitten Dec 2017)

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [DownPaper](https://attack.mitre.org/software/S0186) uses the command line.(Citation: ClearSky Charming Kitten Dec 2017)

Timestamp: 2018-01-16T16:13:52.465Z

--------------------------------------------------------------------------------

Source: MITRE

Risk Level: Medium

Type: relationship

Name: Unnamed

Description: [Magic Hound](https://attack.mitre.org/groups/G0059) has conducted watering-hole attacks through media and magazine websites.(Citation: ClearSky Kittens Back 3 August 2020)

Timestamp: 2022-04-08T18:29:35.467Z

--------------------------------------------------------------------------------

=== RISK DISTRIBUTION ===

High: 53 findings (64.6%)

Medium: 29 findings (35.4%)

Low: 0 findings (0.0%)

=== 5G RELEVANCE ANALYSIS ===

Direct: 4 findings (4.9%)

Indirect: 7 findings (8.5%)

None: 71 findings (86.6%)

PS C:\Users\andre>