E-MIMICS

EXTENDED MALWARE IN MODERN ICS

PROJECT MIMICS

ORIGINAL HYPOTHESES

In 2017, the research was guided by four initial hypotheses.

INFECTED ICS SOFTWARE

Frequently appears online

THREAT DISCOVERY

Aided by public reports

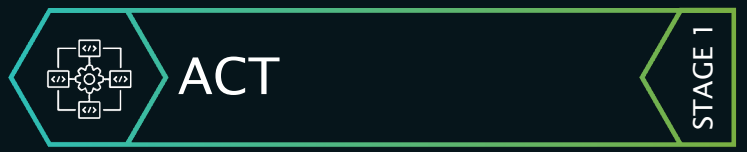
ICS-THEMED MALWARE

Intrusions are not uncommon

SENSITIVE ICS FILES

Submitted to online services by stakeholders and/or products

ICS CYBER KILL CHAIN



DRAGOS

METHODOLOGY: OLD AND NEW

COMPARISON OF INPUT DATA

OLD

- ~3 months of data
- Public data: VirusTotal
- 15,000 total samples
- 3,157 samples returned positive AV results
- Also used Google, DNS data
- Aggregated data using ICS vendors, paths, registries, etc.

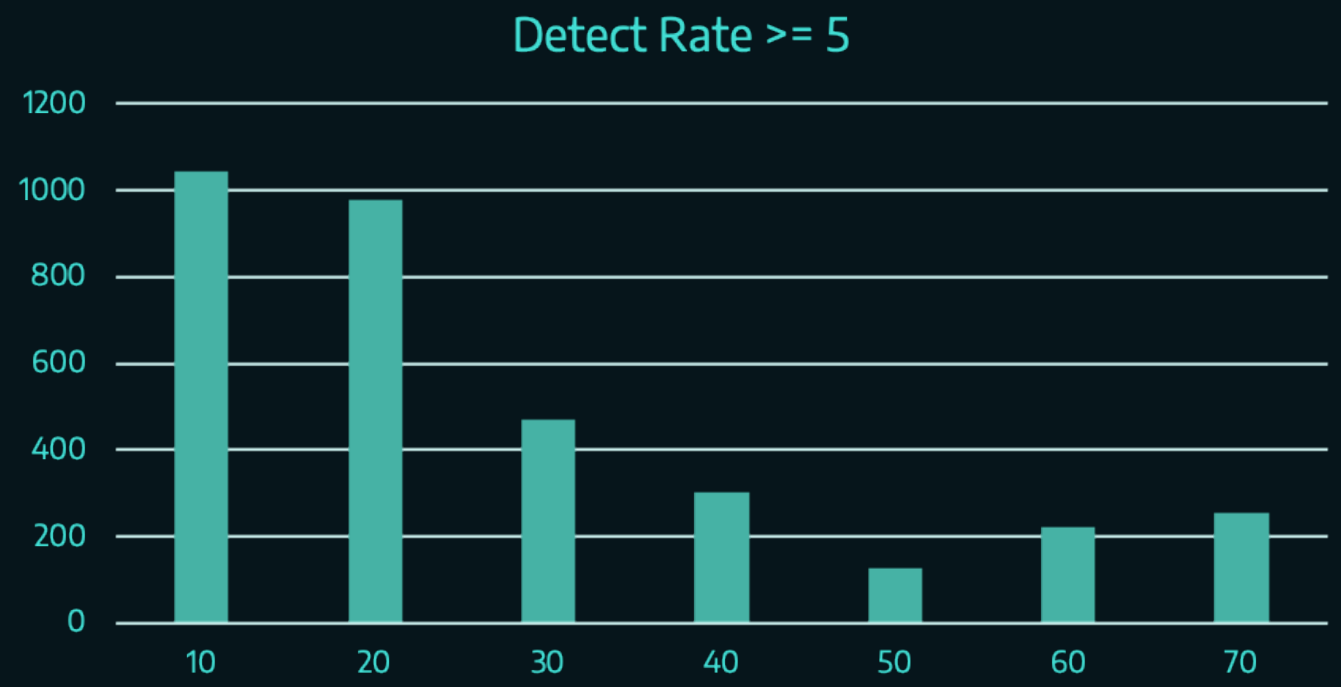
NEW

- ~4 years of data
- Public data: VirusTotal
- Various searches within VT returned a dataset consisting of 359,399 potential malware samples
- Filtered on samples with at least one positive AV detection
- Of these, a random sample of 7,364 VT reports was used to complete the research
- Aggregated data based on ICS vendor only

FINDINGS

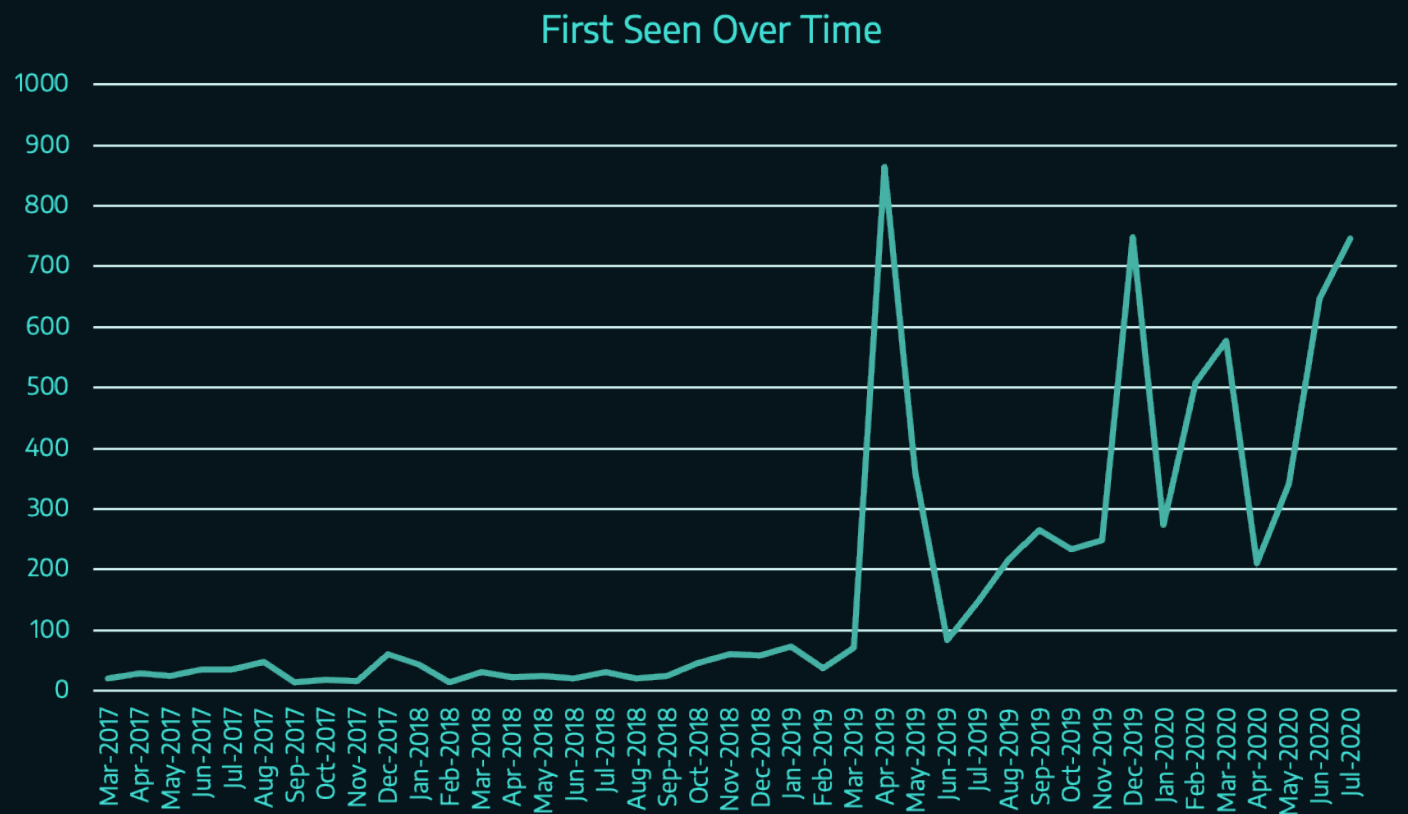
FINDINGS

LIKELIHOOD OF BEING MALICIOUS



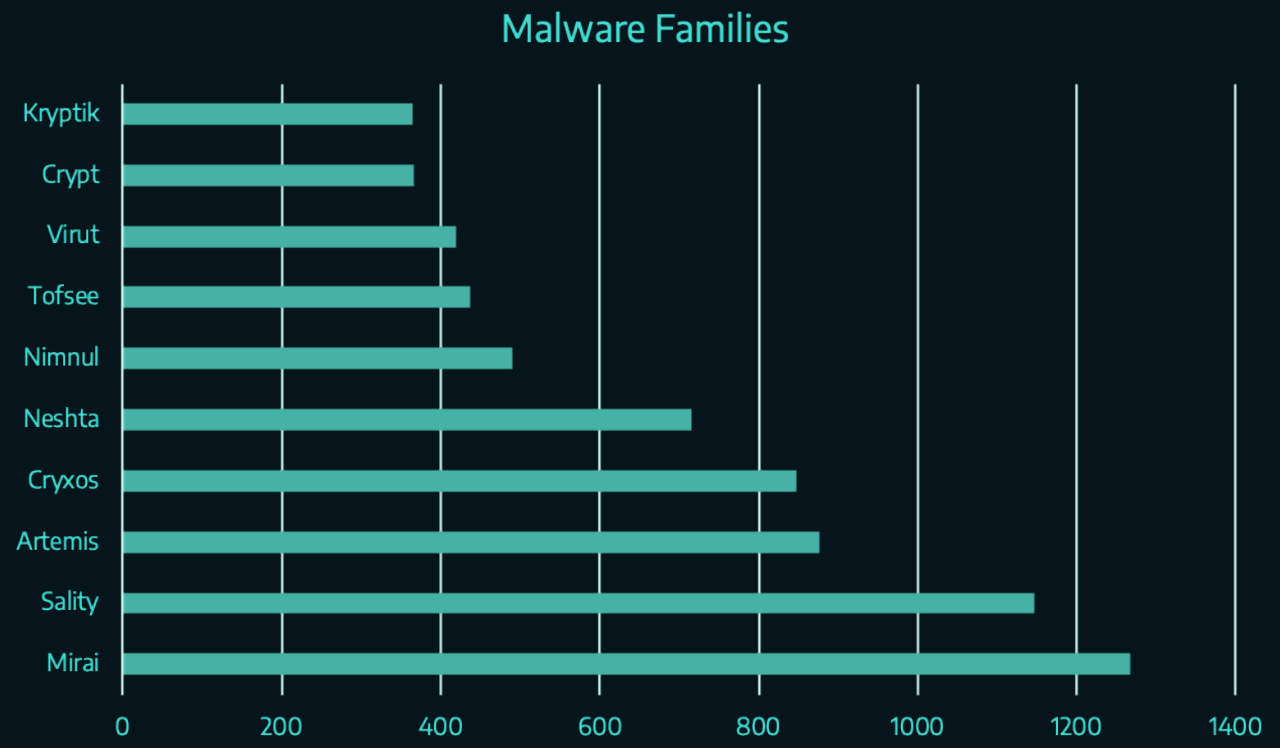
FINDINGS

SUBMISSIONS OVER TIME



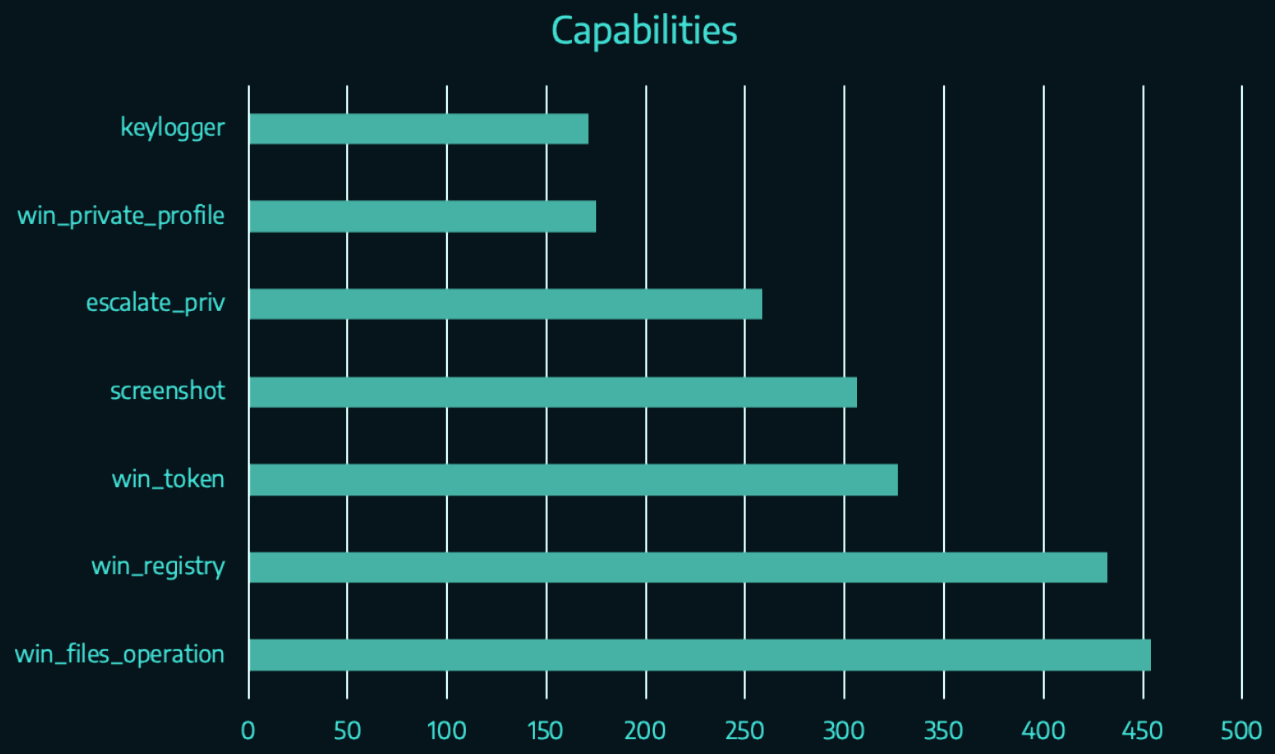
FINDINGS

COMMON FAMILIES



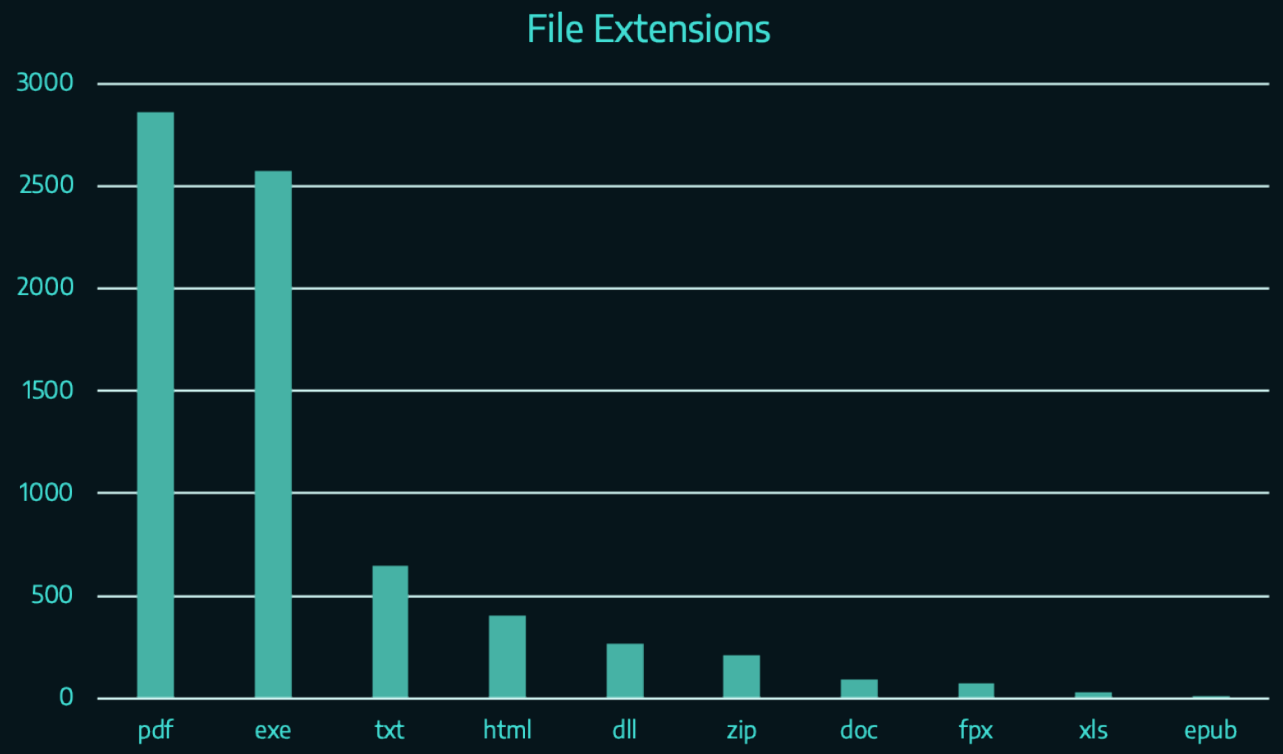
FINDINGS

MALWARE CAPABILITIES



FINDINGS

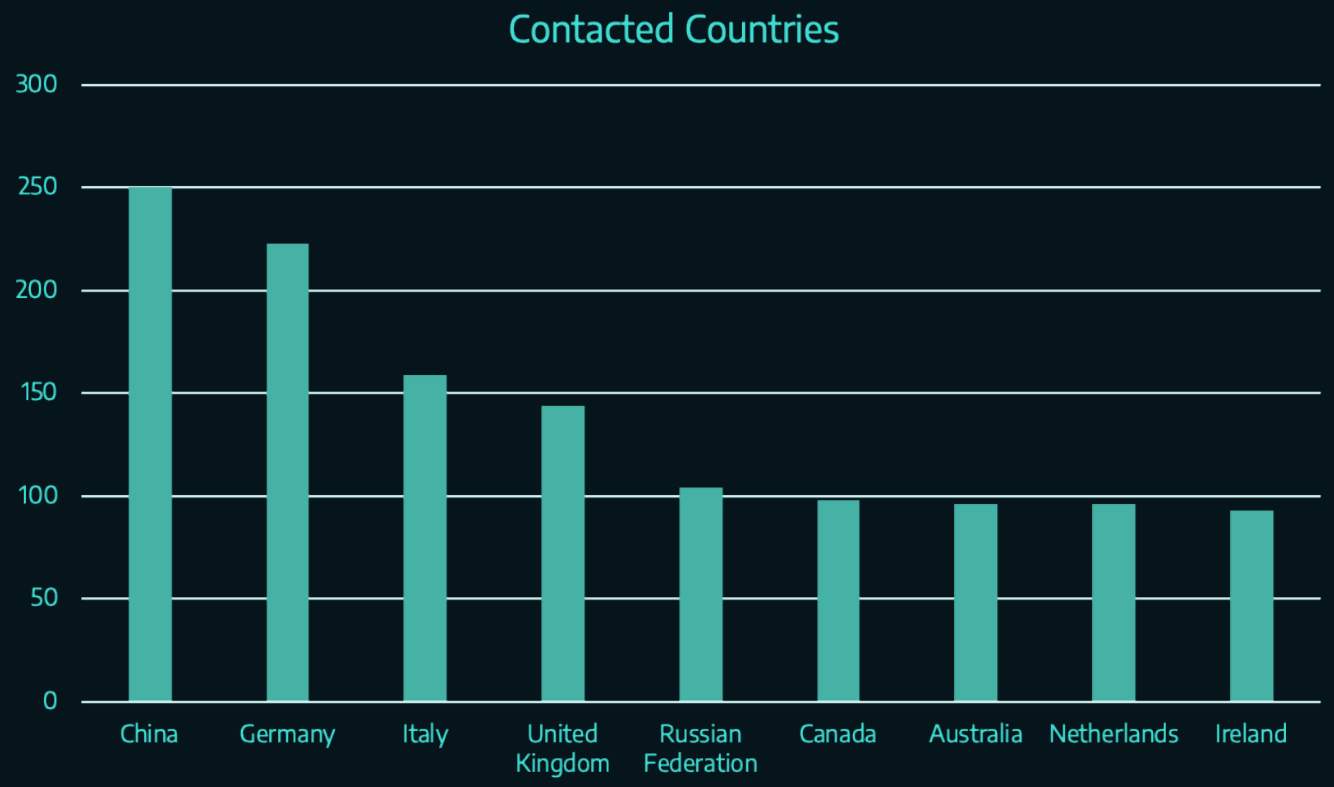
COMMON EXTENSIONS



FINDINGS

CONTACTED COUNTRIES

- US: ~2300



PE INFECTORS YOU SHOULD CARE ABOUT

PE INFECTORS ARE A REAL VECTOR

VIRUT

+ Short for ‘virus’ and ‘trojan’
+ C2 via IRC
+ IRC not required to spread
+ Infects current processes

SALITY

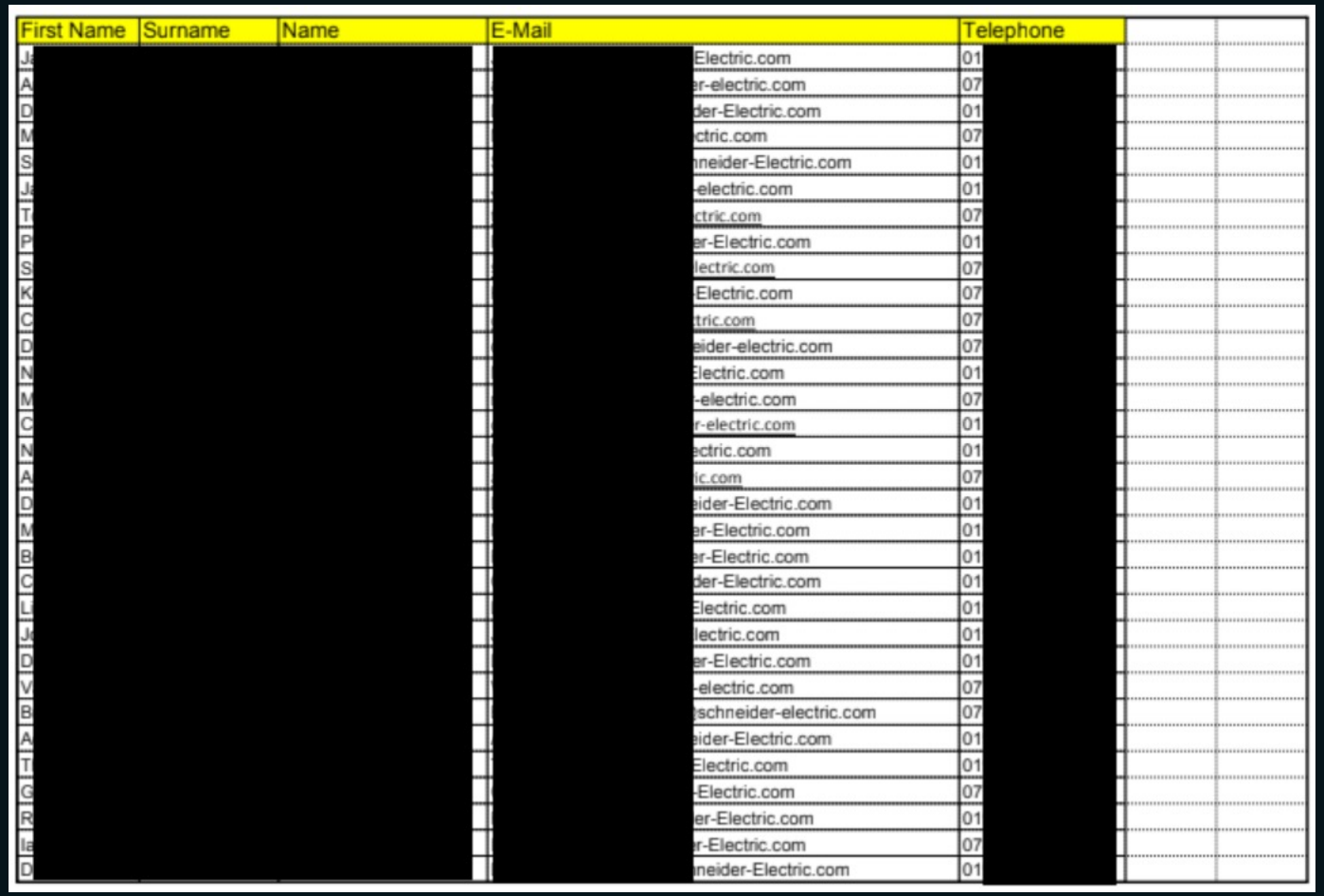
+ Botnet, P2P C2
+ Pay per install
+ Rootkit
+ Infects current processes and executables on all drives: local, network, removable

SENSITIVE FILES

MANY AND VARIED

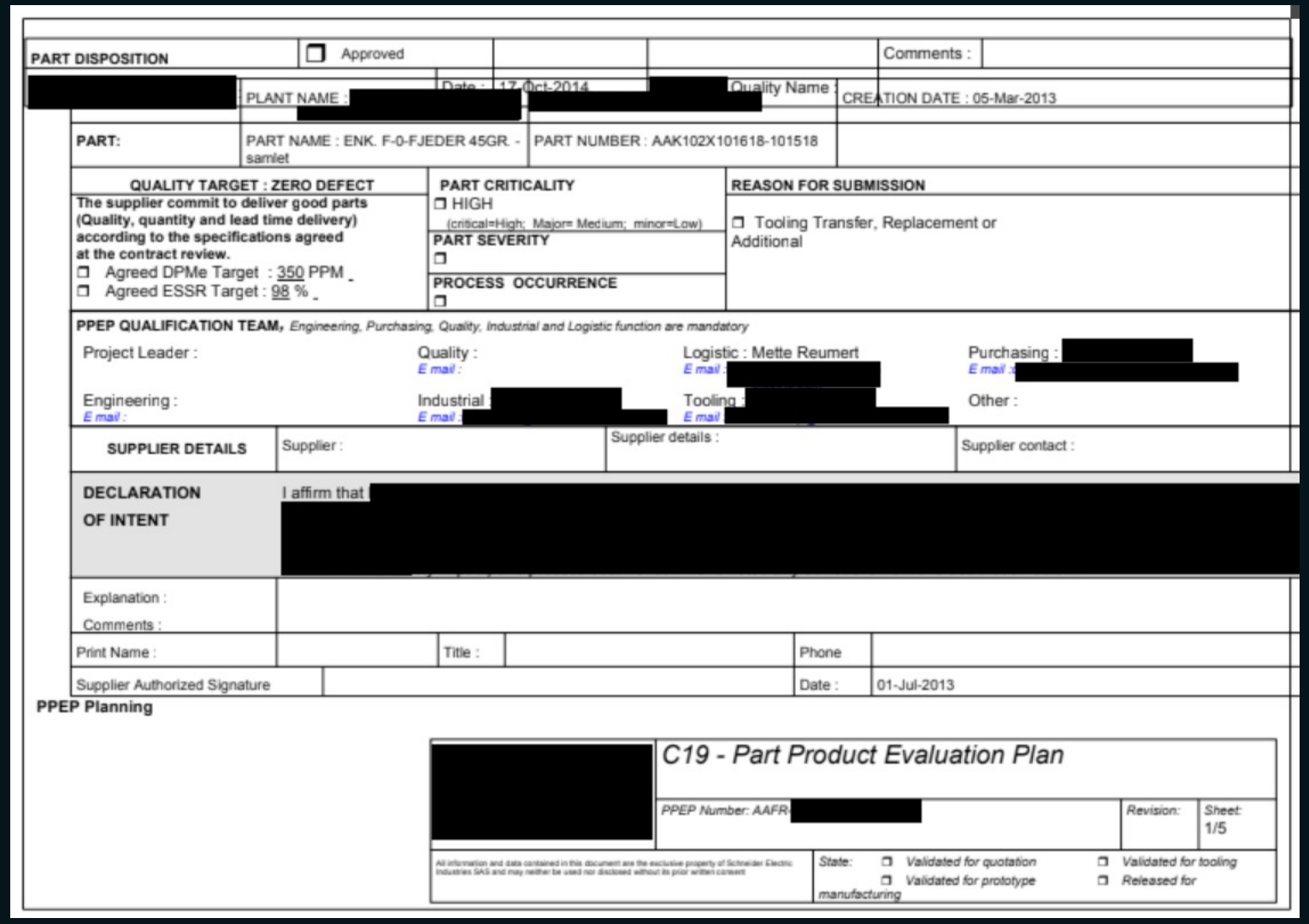
+ Purchase orders
+ Internal contact lists
+ Product evaluation plans
+ Operations reports

INTERNAL CONTACTS



First Name	Surname	Name	E-Mail	Telephone
J	[redacted]	[redacted]	[redacted]Electric.com	01[redacted]
A			[redacted]r-electric.com	07
D			[redacted]der-Electric.com	01
M			[redacted]ctric.com	07
S			[redacted]nneider-Electric.com	01
J			[redacted]-electric.com	01
T			[redacted]ctric.com	07
P			[redacted]er-Electric.com	01
S			[redacted]lectric.com	07
K			[redacted]Electric.com	07
C			[redacted]tric.com	07
D			[redacted]eider-electric.com	07
N			[redacted]Electric.com	01
M			[redacted]-electric.com	07
C			[redacted]r-electric.com	01
N			[redacted]ctric.com	01
A			[redacted]ic.com	07
D			[redacted]ider-Electric.com	01
M			[redacted]er-Electric.com	01
B			[redacted]er-Electric.com	01
C			[redacted]der-Electric.com	01
L			[redacted]Electric.com	01
J			[redacted]lectric.com	01
D			[redacted]er-Electric.com	01
V			[redacted]-electric.com	07
B			[redacted]schneider-electric.com	07
A			[redacted]ider-Electric.com	01
T			[redacted]Electric.com	01
G			[redacted]-Electric.com	07
R			[redacted]er-Electric.com	01
la			[redacted]r-Electric.com	07
D			[redacted]neider-Electric.com	01

PRODUCT EVALUATION PLAN



PART DISPOSITION	❒ Approved			Comments :	
[redacted]	PLANT NAME : [redacted]	Date : 17-Oct-2014	[redacted]	Quality Name : [redacted]	CREATION DATE : 05-Mar-2013
PART:	PART NAME : ENK. F-0-FJEDER 45GR. - samlet		PART NUMBER : AAK102X101618-101518		

QUALITY TARGET : ZERO DEFECT	PART CRITICALITY	REASON FOR SUBMISSION
The supplier commit to deliver good parts (Quality, quantity and lead time delivery) according to the specifications agreed at the contract review. ❒ Agreed DPMe Target : 350 PPM ❒ Agreed ESSR Target : 98 %	❒ HIGH (critical=High; Major= Medium; minor=Low) **PART SEVERITY** ❒ **PROCESS OCCURRENCE** ❒	❒ Tooling Transfer, Replacement or Additional

PPEP QUALIFICATION TEAM, *Engineering, Purchasing, Quality, Industrial and Logistic function are mandatory*

Project Leader :	Quality : *E mail :*	Logistic : Mette Reumert *E mail :* [redacted]	Purchasing : [redacted] *E mail :* [redacted]
Engineering : *E mail :*	Industrial : [redacted] *E mail :* [redacted]	Tooling : [redacted] *E mail :* [redacted]	Other :

SUPPLIER DETAILS	Supplier :	Supplier details :	Supplier contact :

DECLARATION OF INTENT	I affirm that [redacted]
Explanation : Comments :	

Print Name :		Title :		Phone	
Supplier Authorized Signature				Date :	01-Jul-2013

PPEP Planning

[redacted]	*C19 - Part Product Evaluation Plan*		
	PPEP Number: AAFR- [redacted]	*Revision:*	*Sheet:* 1/5
All information and data contained in this document are the exclusive property of Schneider Electric Industries SAS and may neither be used nor disclosed without its prior written consent	*State:* ❒ *Validated for quotation* ❒ *Validated for prototype* ❒ *Validated for tooling* ❒ *Released for manufacturing*		

DRAGOS

DAILY OPERATION SUMMARY REPORT

[redacted]

Oil Production Information System

[redacted] Daily Operations Summary Report

Date 12-Sep-18

[redacted]

Note: Daily allocation of produced volumes is preliminary. Formally reconciled volumes will be issued monthly.

ES&SR				
POB:	113			
LTA's / Injuries Last 24 hrs:	NONE	No. LTA's YTD :	NONE	
High Potential Events/Spills:	None			
SIMOPS :	#928-Nexus General visual inspections. #931 - Nexus NEDC WLR preparations. #932 - Nexus Subsea Riser Cleaning. #933 - Nexus Valve Operations #937 - Barents D3W Injection test			
Plans / Drills etc.:	None			
SEC Impairments:	SEC #	Comments/Mitigation Measures		
	SEC-28 Crane Ope	Fwd Crane rated to 80%		
Safety System Inhibits:	<=30 days	>30 days		
	18	10		
Production/Vessel Inhibits:	<=30 days	>30 days		
	8	14		

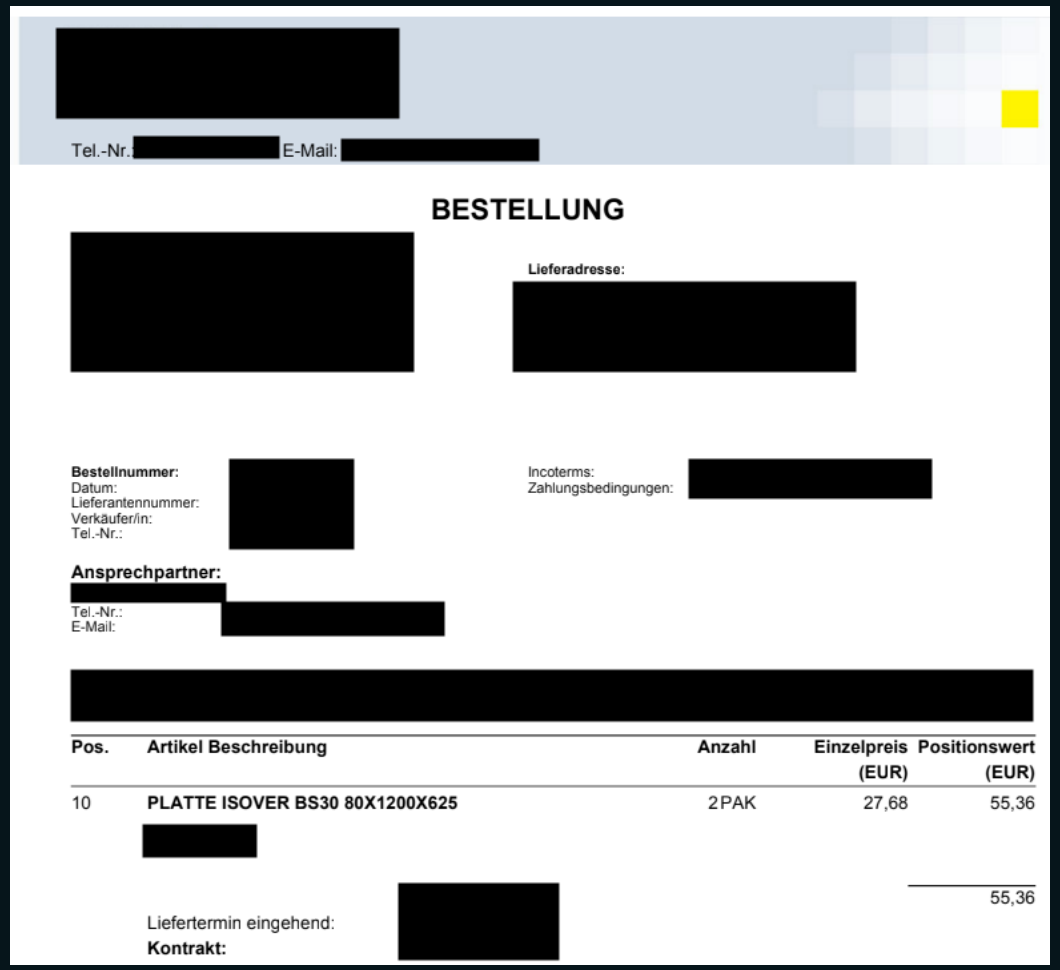
Daily Review	Daily	Cum. MTD	Cum. YTD	Comments
Production Plan Target (Sm3)	6,350			
Net Oil Production (Sm3)	6,002	71,276	1,363,407	Gas Handling constraints.
Target Production Efficiency (%)	95%			
Oil Storage Volume (Sm3)	41,045			Deliverable 33,000 m3. Produced water 3,000 m3.
Gross Gas Production (Sm3)	8,289,542	100,084,363	1,682,354,429	
Net Gas Production (Sm3)	6,596,114	83,069,486	1,372,599,397	
Gas Injection (Sm3)	6,105,259	69,318,760	1,241,839,104	
Gas Lift (Sm3)	1,693,428	17,014,877	309,755,032	
Fuel Gas (Sm3)	464,262	4,429,920	99,037,434	
Flare Gas (Sm3)	26,593	9,320,807	31,722,859	YTD is from 16-Jan. Flare allowance from 16-Jan-18 to 31-Jan-19 is 83.0 million Sm3.
Water Injection (Sm3)	28,194	209,887	5,735,548	
Net Water Production (Sm3)	15,718	168,539		
Gas/Oil Ratio (Sm3/Sm3)	1,098.92	1,165.46		
Water/Oil Ratio (Sm3/Sm3)	2.62	2.36		
Rundown AI-210023 BS&W (%)	0.3784	0.3395		
Rundown LAB KF Water (%)	0.2000	0.1988		
GVP (kpaa)	49.80	50.58		Corresponding RVP = 41.57 kPaa
Discharges				NOTE: Produced Water Discharge using backup calculation. Sum of meters FI-200149 and FI-200150
Produced Water Discharge (Sm3)	15,734	168,175	3,372,507	NOTE: Discharge Volumes are preliminary and are formally reconciled in Monthly Compliance Report
Produced Water Discharge Qlty (mg/L)	7.8			24 hr avg (PM - AM)
Produced Water Discharge Qlty (mg/L)	7.9	10.4	11.7	24 hr avg (AM - PM) and 30 day rolling avg - Using Lab Analysis
Slop Tank Drain Water Quality (mg/L)	Invalid	Invalid	0.6	Using Lab Analysis
Slop Tank Level (m3)	2,973			Preliminary number, for monitoring purpose only
Field Prod. Allocation Factors				
Oil	0.96267	0.97921		
Gas	0.94446	0.97860		
Water	1.11979	1.15550		
Rundown Meter Correction Factor	1.000			

DRAGOS

DAILY OPERATION SUMMARY REPORT

Key Equipment Status				
System	**Status**	**Unavailable since?**	**Expected Availability Date**	**Comments**
LP Compressor	Running			Run 24 hrs
MP Compressor	Running			Run 24 hrs
HP1 Compressor	Running			Run 24 hrs
HP2 Compressor	Running			Run 24 hrs
Main Power Generator "A"	Running			Run 24 hrs
Main Power Generator "B"	Running			Run 24 hrs
Key Services Generator "A"	Available			
Key Services Generator "B"	Available			
Water Injection Pump "A"	Available			
Water Injection Pump "B"	Running			Run 24 hrs
Water Injection Pump "C"	Running			Run 24 hrs
Gas Dehydration System	Running			Run 24 hrs
Framo Hydraulic System	Running			
Emergency Generator	Available			
HC Blanket Gas and Recovery	Unavailabl		16-Sep	Blower discharge XXV not fully closing. Condensate accumulation identified in discharge piping. Start up procedure being modified.
IGG #1	Available			Run 13.77 hrs SD 00:00 - 08:19 22:06 - 00:00
IGG #2	Available			
Port Boiler	Running			Run 24 hrs
Stbd Boiler	Unavailable	12-Sep	NA	Run 0.18 hrs SD 00:00 - 03:47 03:58 - 00:00 Depressured and isolated for 52 wk inspection

ORDER FORMS



[redacted]

Tel.-Nr. [redacted] E-Mail: [redacted]

BESTELLUNG

[redacted]

Lieferadresse:

[redacted]

Bestellnummer: [redacted]
Datum:
Lieferantennummer:
Verkäufer/in:
Tel.-Nr.:

Incoterms:
Zahlungsbedingungen: [redacted]

Ansprechpartner:
[redacted]
Tel.-Nr.:
E-Mail: [redacted]

[redacted]

Pos.	Artikel Beschreibung	Anzahl	Einzelpreis (EUR)	Positionswert (EUR)
10	**PLATTE ISOVER BS30 80X1200X625**	2PAK	27,68	55,36
	[redacted]			

55,36

Liefertermin eingehend: [redacted]
Kontrakt:

KEY TAKEAWAYS

- ICS-themed malware is becoming more common
- Think not just about the threats, but their behaviours and TTPs when implementing your defence strategies
- Understand connectivity and ingress / egress to your networks, do complete due diligence if allowing any remote connections
- Understand that you're more likely to be infected, targeted or opportunistically, than you might think
- Virut and others like it are capable of lowering your defences

FUTURE RESEARCH

WHAT SHOULD WE DO NEXT?

- Further research on the malware submissions (i.e. reverse engineering)
- Number of sensitive data files submitted
- Look at project files specifically
- A longitudinal study using multiple data points on a frequent basis (i.e. monthly)
- Utilize additional data sources, like Shodan and others

THANK YOU

DRAGOS

SENOKA@DRAGOS.COM
DRAGOS.COM