

Fra idé til Ransomware

Business Development «on the dark side»



Conscia
Secure progress

En stille kveld utenfor Kraków (2015)



En stille kveld utenfor Kraków

- En datamaskin og nysgjerrighet
- Noe fleksibel moral
- Lekket e-postliste
- Med penger som motiv
- Automatisert utsending phishing-e-poster
- Innhenting av sensitiv informasjon
- En kodesnutt blir bygget



```
80
81 # --- module: phishing_sim.py (main) ---
82 def main():
83     parser = argparse.ArgumentParser(description="Simulated Phishing Script v01e")
84     parser.add_argument('--input', required=True, help='Path to input CSV file (name,email)')
85     parser.add_argument('--output', required=True, help='Path to output log CSV')
86     parser.add_argument('--email-template', required=True, help='Path to HTML email template')
87     parser.add_argument('--email-css', help='Optional CSS file to inline in the email')
88     parser.add_argument('--email-service', default='GenericMail', help='Email service name (e.g., Google, Microsoft 365)')
89     parser.add_argument('--landing-url', help='Optional landing page URL to inject into template')
90     parser.add_argument('--simulate-mfa-bypass', action='store_true', help='Simulate MFA bypass elements in template')
91     args = parser.parse_args()
92
93     targets = load_targets(args.input)
94     email_template = load_template(args.email_template)
95
96     results = []
97     for target in targets:
98         email_body = generate_phishing_email(
99             target["name"],
100             email_template,
101             css_path=args.email_css,
102             landing_url=args.landing_url,
103             simulate_mfa_bypass=args.simulate_mfa_bypass
104         )
105         success = send_email_mock(target, email_body, args.email_service)
106         results.append({
107             "email": target["email"],
108             "status": "Sent" if success else "Failed",
109             "timestamp": datetime.utcnow().isoformat()
110         })
111
112     write_log(results, args.output)
113     print(f"\n[INFO] Kampanjeloggen er lagret i {args.output}")
114
115 if __name__ == "__main__":
116     main()
117
```



```
55         </div>
56         """
57         email_body += mfa_html
58
59         return f"<html><head>{css_inline}</head><body>{email_body}</body></html>"
60
61 # --- module: sender.py ---
62 def send_email_mock(target, content, service_name):
63     """
64     Simulates sending an email. In a real system, this would send via SMTP or API.
65     """
66     print(f"[MOCK SEND] To: {target['email']} | From: alerts@{service_name.lower().replace(' ', '')}.com")
67     return True
68
69 # --- module: logger.py ---
70 def write_log(results, output_file):
71     """
72     Writes the result of each email to a CSV log file.
73     """
74     with open(output_file, mode='w', newline='') as logfile:
75         fieldnames = ['email', 'status', 'timestamp']
76         writer = csv.DictWriter(logfile, fieldnames=fieldnames)
77         writer.writeheader()
78         for result in results:
79             writer.writerow(result)
80
81 # --- module: phishing_sim.py (main) ---
82 def main():
83     parser = argparse.ArgumentParser(description="Simulated Phishing Script v01e")
84     parser.add_argument('--input', required=True, help='Path to input CSV file (name,email)')
85     parser.add_argument('--output', required=True, help='Path to output log CSV')
86     parser.add_argument('--email-template', required=True, help='Path to HTML email template')
87     parser.add_argument('--email-css', help='Optional CSS file to inline in the email')
88     parser.add_argument('--email-service', default='GenericMail', help='Email service name (e.g., Google, Microsoft 365)')
89     parser.add_argument('--landing-url', help='Optional landing page URL to inject into template')
90     parser.add_argument('--simulate-mfa-bypass', action='store_true', help='Simulate MFA bypass elements in template')
91     args = parser.parse_args()
92
93     targets = load_targets(args.input)
94     email_template = load_template(args.email_template)
95
96     results = []
```

```
22     },
23     return targets
24
25 # --- module: templates.py ---
26 def load_template(template_path):
27     """
28     Loads an HTML template from file.
29     """
30     if not os.path.exists(template_path):
31         raise FileNotFoundError(f"Template not found: {template_path}")
32     with open(template_path, 'r', encoding='utf-8') as file:
33         return file.read()
34
35 def generate_phishing_email(name, email_template, css_path=None, landing_url=None, simulate_mfa_bypass=False):
36     """
37     Generates a phishing email using a template, optional CSS, optional landing page URL,
38     and optional MFA bypass simulation indicator.
39     """
40     css_inline = ""
41     if css_path and os.path.exists(css_path):
42         with open(css_path, 'r', encoding='utf-8') as css_file:
43             css_inline = f"<style>{css_file.read()}</style>"
44
45     email_body = email_template.replace("{{name}}", name)
46     if landing_url:
47         email_body = email_body.replace("{{landing_url}}", landing_url)
48
49     if simulate_mfa_bypass:
50         mfa_html = """
51         <div style='margin-top:20px;padding:10px;border:1px solid #ccc;background:#f9f9f9;'>
52             <p><strong>Du kan også godkjenne innloggingen via mobilen din:</strong></p>
53             <img src='https://example.com/qr-placeholder.png' alt='QR-kode for MFA' width='150'/>
54             <p style='font-size:small;color:#666;'>Denne koden utløper om 2 minutter.</p>
55         </div>
56         """
57         email_body += mfa_html
58
59     return f"<html><head>{css_inline}</head><body>{email_body}</body></html>"
60
61 # --- module: sender.py ---
62 def send_email_mock(target, content, service_name):
63     """
```

```
1 import csv
2 import argparse
3 from datetime import datetime
4 import os
5
6 # Version: 02a
7 # Modularized phishing simulation script with MFA bypass
8
9 # --- module: targets.py ---
10 def load_targets(input_file):
11     """
12     Loads target emails and names from a CSV file.
13     Expects columns: name,email
14     """
15     targets = []
16     with open(input_file, newline='') as csvfile:
17         reader = csv.DictReader(csvfile)
18         for row in reader:
19             targets.append({
20                 "name": row["name"],
21                 "email": row["email"]
22             })
23     return targets
24
25 # --- module: templates.py ---
26 def load_template(template_path):
27     """
28     Loads an HTML template from file.
29     """
30     if not os.path.exists(template_path):
31         raise FileNotFoundError(f"Template not found: {template_path}")
32     with open(template_path, 'r', encoding='utf-8') as file:
33         return file.read()
34
35 def generate_phishing_email(name, email_template, css_path=None, landing_url=None, simulate_mfa_bypass=False):
36     """
37     Generates a phishing email using a template, optional CSS, optional landing page URL,
38     and optional MFA bypass simulation indicator.
```

```
80
81 # --- module: phishing_sim.py (main) ---
82 def main():
83     parser = argparse.ArgumentParser(description="Simulated Phishing Script v01e")
84     parser.add_argument('--input', required=True, help='Path to input CSV file (name,email)')
85     parser.add_argument('--output', required=True, help='Path to output log CSV')
86     parser.add_argument('--email-template', required=True, help='Path to HTML email template')
87     parser.add_argument('--email-css', help='Optional CSS file to inline in the email')
88     parser.add_argument('--email-service', default='GenericMail', help='Email service name (e.g., Google, Microsoft 365)')
89     parser.add_argument('--landing-url', help='Optional landing page URL to inject into template')
90     parser.add_argument('--simulate-mfa-bypass', action='store_true', help='Simulate MFA bypass elements in template')
91     args = parser.parse_args()
92
93     targets = load_targets(args.input)
94     email_template = load_template(args.email_template)
95
96     results = []
97     for target in targets:
98         email_body = generate_phishing_email(
99             target["name"],
100             email_template,
101             css_path=args.email_css,
102             landing_url=args.landing_url,
103             simulate_mfa_bypass=args.simulate_mfa_bypass
104         )
105         success = send_email_mock(target, email_body, args.email_service)
106         results.append({
107             "email": target["email"],
108             "status": "Sent" if success else "Failed",
109             "timestamp": datetime.utcnow().isoformat()
110         })
111
112     write_log(results, args.output)
113     print(f"\n[INFO] Kampanjeloggen er lagret i {args.output}")
114
115 if __name__ == "__main__":
116     main()
117
```

Fra script til tjeneste



Fra script til tjeneste

- Et enkelt Python script blir en suksess
- Prosessen tar tid og krever oppdateringer
- Hva om dette automatiseres?
- Kan automasjonen tilbys som tjeneste?
- En ide om Phishing as a Service blir født.

Rammeverk



Rammeverk

- Valg av målgruppe



Rammeverk

- Valg av målgruppe
- Innsamling av informasjon



Rammeverk

- Valg av målgruppe
- Innsamling av informasjon
- Valg av metode



Rammeverk

- Valg av målgruppe
- Innsamling av informasjon
- Valg av metode
- Forberedelse av infrastruktur



Rammeverk

- Valg av målgruppe
- Innsamling av informasjon
- Valg av metode
- Forberedelse av infrastruktur
- Utforming av innhold



Rammeverk

- Valg av målgruppe
- Innsamling av informasjon
- Valg av metode
- Forberedelse av infrastruktur
- Utforming av innhold
- Testing



Rammeverk

- Valg av målgruppe
- Innsamling av informasjon
- Valg av metode
- Forberedelse av infrastruktur
- Utforming av innhold
- Testing
- Planlegg og iverksett

Phishing as a Service

Phishing as a Service

- Skybasert plattform
- Phishing-maler og automasjon mot betaling
- Abonentene sparer tid og tjener penger raskere
- Det gjør også Andrzej
- Forretningsmulighetene øker

Phishing as a Service

- Automatiserte krypto-betalingsystemer
- Anonyme transaksjoner
- Reduserer rettslig risiko
- Kundeopplevelse

Hva mer?



Hva mer?

- Mer enn phishing?
- Hva med Phishing-Awareness-Training-Service?
- Kan vi droppe en agent med payload?
- Kan vi eksfiltrere data?
- Kan vi kryptere data?
- Ransomware-kode
- Integrasjon med phishing as a service plattform

Utvikling av Ransomware as a Service



Utvikling av Ransomware as a Service

- Marked place
- «Initial access» og «persistence brokers»
- «Discovered data» og «Lateral movements brokers»
- «Collection og exfiltrated data brokers»
- «Ransomware brokers»

RaaS - Næringskjede

RaaS - Næringskjede

- Utviklere (Core Ransomware Developers)



RaaS - Næringskjede

- Utviklere (Core Ransomware Developers)
- Initial Access Brokers (IABs)



RaaS - Næringskjede

- Utviklere (Core Ransomware Developers)
- Initial Access Brokers (IABs)
- Loader- og dropper-operatører



RaaS - Næringskjede

- Utviklere (Core Ransomware Developers)
- Initial Access Brokers (IABs)
- Loader- og dropper-operatører
- Recon og lateral movement operatører





RaaS - Næringskjede

- Utviklere (Core Ransomware Developers)
- Initial Access Brokers (IABs)
- Loader- og dropper-operatører
- Recon og lateral movement operatører
- Eksfiltrasjonsspesialister





RaaS - Næringskjede

- Utviklere (Core Ransomware Developers)
- Initial Access Brokers (IABs)
- Loader- og dropper-operatører
- Recon og lateral movement operatører
- Eksfiltrasjonsspesialister
- Kryptering og trigger-operatører



RaaS - Næringskjede

- Utviklere (Core Ransomware Developers)
- Initial Access Brokers (IABs)
- Loader- og dropper-operatører
- Recon og lateral movement operatører
- Eksfiltrasjonsspesialister
- Kryptering og trigger-operatører
- Negotiators og Chat-operatører



RaaS - Næringskjede

- Utviklere (Core Ransomware Developers)
- Initial Access Brokers (IABs)
- Loader- og dropper-operatører
- Recon og lateral movement operatører
- Eksfiltrasjonsspesialister
- Kryptering og trigger-operatører
- Negotiators og Chat-operatører
- Marketplace / Infrastrukturleverandører



RaaS - Næringskjede

- Utviklere (Core Ransomware Developers)
- Initial Access Brokers (IABs)
- Loader- og dropper-operatører
- Recon og lateral movement operatører
- Eksfiltrasjonsspesialister
- Kryptering og trigger-operatører
- Negotiators og Chat-operatører
- Marketplace / Infrastrukturleverandører
- Beting og hvitvasking



RaaS - Næringskjede

- Utviklere (Core Ransomware Developers)
- Initial Access Brokers (IABs)
- Loader- og dropper-operatører
- Recon og lateral movement operatører
- Eksfiltrasjonsspesialister
- Kryptering og trigger-operatører
- Negotiators og Chat-operatører
- Marketplace / Infrastrukturleverandører
- Beting og hvitvasking
- Analyse og evaluering



RaaS - Næringskjede

- Utviklere (Core Ransomware Developers)
- Initial Access Brokers (IABs)
- Loader- og dropper-operatører
- Recon og lateral movement operatører
- Eksfiltrasjonsspesialister
- Kryptering og trigger-operatører
- Negotiators og Chat-operatører
- Marketplace / Infrastrukturleverandører
- Beting og hvitvasking
- Analyse og evaluering
- Samarbeidsformer og flyt



RaaS utvikling i 2025



RaaS utvikling i 2025

- Modulære AI-verktøy





RaaS utvikling i 2025

- Modulære AI-verktøy
- Automatiserte ChatOps





RaaS utvikling i 2025

- Modulære AI-verktøy
- Automatiserte ChatOps
- Multi-extortion campaigns





RaaS utvikling i 2025

- Modulære AI-verktøy
- Automatiserte ChatOps
- Multi-extortion campaigns
- Zero Trust-bypass kits





RaaS utvikling i 2025

- Modulære AI-verktøy
- Automatiserte ChatOps
- Multi-extortion campaigns
- Zero Trust-bypass kits
- Fordelsprogram

Andrzej RaaS



Login

admin

Logg inn



Dashboard

Kommando-senter Kampanjer LiveMap Accounts Marketplace Knowledge

Aktive kampanjer

5 pågående, 2 i pause, 1 nylig avsluttet.

Infiserte enheter (siste 24t)

37 nye infeksjoner sporet i 8 land.

Eksfiltrert data

Ca. 128 GB eksfiltrert fra 12 mål denne uken.

Omsetning (estimert)

\$238,000 hittil denne måneden.

Mest aktive moduler

WinDropper, CryptoLocker XT,
BlackNegotiator AI

Tilgjengelige initial accesses

24 unike tilgangspunkter listet i markedet.



Kommando-senter

[Dashboard](#) [Kampanjer](#) [LiveMap](#) [Accounts](#) [Marketplace](#) [Knowledge](#)

Pågående operasjoner

ID	Lokasjon	Metode	Status	Alvorlighetsgrad	Tidspunkt
OP-0921	Oslo	Phishing + Loader	Aktiv	Høy	08:43
OP-1543	Berlin	VPN Access + Cobalt Strike	Beveger seg lateralt	Kritisk	08:49
OP-2380	New York	Initial Access Broker + Ransomware	Kryptert	Kritisk	08:52
OP-4432	Tokyo	Zero-Day Exploit + Loader	Under utforskning	Middels	08:56
OP-3107	Moskva	Spear Phishing + InfoStealer	Data eksfiltrert	Høy	09:01
OP-5119	København	MalSpam + Custom Payload	Ferdigstilt	Middels	09:05

Kampanjeoversikt

[Dashboard](#) [Kommando-senter](#) [LiveMap](#) [Accounts](#) [Marketplace](#) [Knowledge](#)

Aktive og tidligere kampanjer

Navn	Målgruppe	Startdato	Status	Resultat
Frostbite	Nordiske SMB-bedrifter	2024-12-01	Aktiv	13 infeksjoner
Nightfox	Amerikanske finansinstitusjoner	2025-01-15	Under analyse	7 kompromittert
Redvine	EU helsesektor	2024-11-20	Ferdigstilt	21 eksfiltrert
Steelshadow	Asiatiske teknologiselskaper	2025-03-03	Pause	4 avbrutt
PhantomWire	Globale logistikkleverandører	2025-02-08	Aktiv	5 løsepengekrav



Live-overvåking – Globale mål og infeksjoner



Oslo: 2 pågående infeksjoner

Berlin: 3 mål under analyse

New York: 4 mål kompromittert

Tokyo: 3 løsepengekrav sendt

Moskva: 5 aktive kampanjer

Rio de Janeiro: 2 aktive payloads

Sydney: Nytt mål identifisert

København: 1 løsepenger mottatt



Brukeradministrasjon

[Dashboard](#) [Kommando-senter](#) [Kampanjer](#) [LiveMap](#) [Marketplace](#) [Knowledge](#)

Aktive kontoer og roller

Brukernavn	Rolle	Aktivitet	Status	Sist innlogget
rootmaster	Administrator	Opprettet kampanje "Frostbite"	Aktiv	09:12
aff_dragon	Affiliate	Distribuerte loader til 3 mål	Aktiv	09:00
cryptodev	Modul-utvikler	Oppdaterte CryptoLocker XT	Aktiv	08:48
stealer_ops	Broker	Eksfiltrerte data fra NY-OP-2380	Inaktiv	07:23
neg_ai	Negotiator	Forhandlet løsepenger for 2 mål	Aktiv	08:55
iab_trader	IAB	La til 5 nye tilgangspunkter	Aktiv	09:05

RaaS Marketplace

[Dashboard](#) [Kommando-senter](#) [Kampanjer](#) [LiveMap](#) [Accounts](#) [Knowledge](#)

Tilgjengelige tjenester og moduler

Søk etter modul eller beskrivelse...

Navn	Beskrivelse	Type	Pris	Status
SilentAccess v3	Tilgang til 50+ SMB-nettverk via RDP og VPN.	Initial Access	\$2,400	På lager
CrypterX PRO	AV-omgåelse for PE-payloads, ukentlig oppdatert.	Crypter	\$1,250	Oppdatert
StealthLoader	Modul for stealth-distribusjon i AD-domener.	Loader	\$980	På lager
LeakHunter	Broker for eksfiltrert data, anonym distribusjon.	Data Broker	10% av salgsverdi	Begrenset
BlackNegotiator AI	Automatisert løsepengeforhandling.	Negotiation Service	\$300 pr forhandling	Tilgjengelig
ShadowBackup Scanner	Scanner og fjerner gjenopprettingspunkter.	Persistence Tool	\$800	Aktiv
CredHarvest ELITE	Passorduthenting via Outlook og browser.	Credential Dumper	\$720	Tilgjengelig

SilentAccess v3	Tilgang til 50+ SMB-nettverk via RDP og VPN.	Initial Access	\$2,400	På lager
CrypterX PRO	AV-omgåelse for PE-payloads, ukentlig oppdatert.	Crypter	\$1,250	Oppdatert
StealthLoader	Modul for stealth-distribusjon i AD-domener.	Loader	\$980	På lager
LeakHunter	Broker for eksfiltrert data, anonym distribusjon.	Data Broker	10% av salgsverdi	Begrenset
BlackNegotiator AI	Automatisert løsepengeforhandling.	Negotiation Service	\$300 pr forhandling	Tilgjengelig
ShadowBackup Scanner	Scanner og fjerner gjenopprettingspunkter.	Persistence Tool	\$800	Aktiv
CredHarvest ELITE	Passorduthenting via Outlook og browser.	Credential Dumper	\$720	Tilgjengelig
NetReconPro	Verktøy for kartlegging og pivoting internt.	Recon Tool	\$1,100	Oppdatert
WinDropper	Dropper for Windows payloads med evasion.	Dropper	\$460	Tilgjengelig
LinuxDropper	Cross-platform stealth dropper for ELF-binaries.	Dropper	\$620	Ny
VPNStealer	Stjeler VPN-profiler fra klienter.	Information Stealer	\$250	På lager
PersistenceKeeper	Registreringsbasert persistens.	Persistence Tool	\$190	Tilgjengelig
CryptoLocker XT	Klassisk ransomware med kryptering og GUI.	Ransomware	\$1,950	Oppdatert
DataExfil Pro	Eksfiltrasjon over HTTP/HTTPS via proxy-chain.	Exfiltration Tool	\$1,500	Tilgjengelig
...	...	...	...	...



Knowledge Base

[Dashboard](#) [Kommando-senter](#) [Kampanjer](#) [LiveMap](#) [Accounts](#) [Marketplace](#)

Dokumenterte metoder, trender og teknikker

Initial Access Brokers (IABs)

Selger tilgang til kompromitterte nettverk. Nøkkelaktører i distribusjonskjeden for RaaS.

Double Extortion

Kombinerer datakryptering med trusler om publisering av stjålne data.

Payload Leveraging

Bruk av trinnvis lastede moduler: loader, krypterer, stealer osv.

Angriper via tredjeparts programvare eller leverandører.

Negotiation-as-a-Service (NaaS)

Automatiserte eller menneskelige forhandlere for løsepengekrav.

MalSpam Campaigns

Massedistribusjon av ondsinnede e-poster for initial fotfeste.

Living Off the Land (LOTL)

Bruk av innebygde verktøy som PowerShell for å unngå deteksjon.

Credential Harvesting

Stjeler brukernavn og passord via keyloggers eller browser extractors.

Command and Control (C2)



Dashboard

Kommando-senter Kampanjer LiveMap Accounts Marketplace Knowledge

Aktive kampanjer

5 pågående, 2 i pause, 1 nylig avsluttet.

Infiserte enheter (siste 24t)

37 nye infeksjoner sporet i 8 land.

Eksfiltrert data

Ca. 128 GB eksfiltrert fra 12 mål denne uken.

Omsetning (estimert)

\$238,000 hittil denne måneden.

Mest aktive moduler

WinDropper, CryptoLocker XT,
BlackNegotiator AI

Tilgjengelige initial accesses

24 unike tilgangspunkter listet i markedet.

Q1 2025 – 126% vekst i utpressing hvor
ofre publiseres offentlig

<https://blog.checkpoint.com/research/the-state-of-ransomware-in-the-first-quarter-of-2025-a-126-increase-in-ransomware-yoy/>

Andrzej's historie er fiktiv



Conscia

Secure progress

Conscia Norge AS

leb@conscia.no