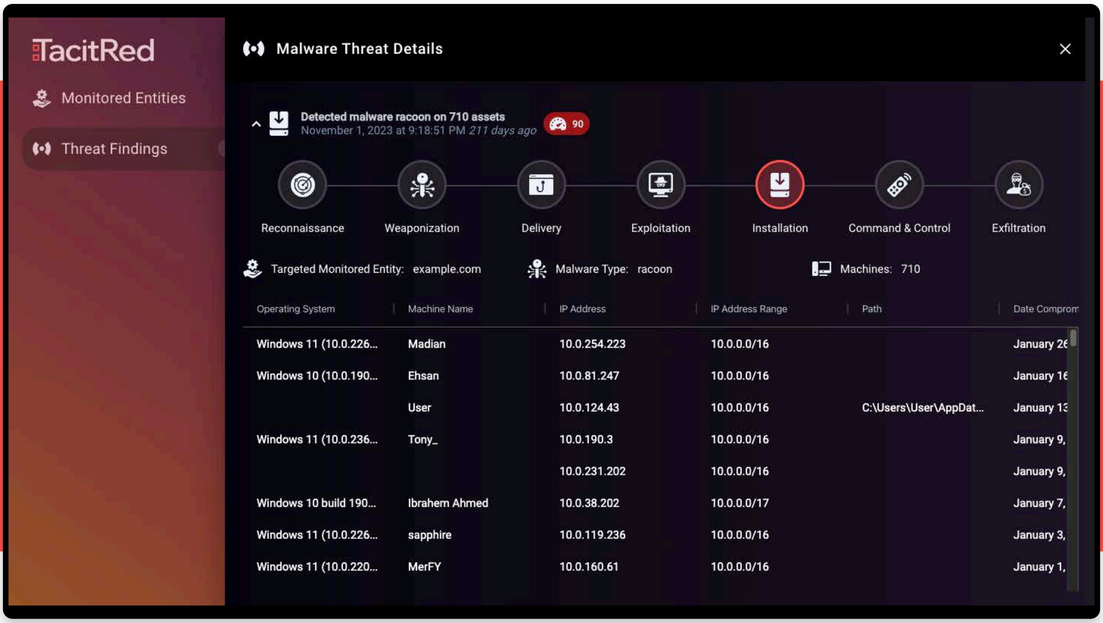
Accurate Cyber Insurance Underwriting in a Complex World

Phishing and social engineering are the #1 cause of ransomware in the world because someone always clicks the link, runs the malware, or disables their multifactor authentication.

In one high-profile breach, threat actors accessed privileged accounts with stolen credentials and socially engineered their way to more critical network resources.

When people are the target, accurate cyber underwriting seems an almost impossible problem. But a solution has arrived.

We've developed intelligence collections and analysis to mitigate social engineering breaches. The TacitRed cyber intelligence platform converts billions of streaming, threat datapoints into actionable intelligence—giving underwriters a fighting chance.



Detected malware racoon on 710 assets
November 1, 2023 at 9:18:51 PM *211 days ago*

Targeted Monitored Entity: example.com
Malware Type: racoon
Machines: 710

Operating System	Machine Name	IP Address	IP Address Range	Path	Date Comprom
Windows 11 (10.0.226...	Madian	10.0.254.223	10.0.0.0/16		January 26
Windows 10 (10.0.190...	Ehsan	10.0.81.247	10.0.0.0/16		January 16
	User	10.0.124.43	10.0.0.0/16	C:\Users\User\AppDat...	January 13
Windows 11 (10.0.236...	Tony_	10.0.190.3	10.0.0.0/16		January 9,
		10.0.231.202	10.0.0.0/16		January 9,
Windows 10 build 190...	Ibrahem Ahmed	10.0.38.202	10.0.0.0/17		January 7,
Windows 11 (10.0.226...	sapphire	10.0.119.236	10.0.0.0/16		January 3,
Windows 11 (10.0.220...	MerFY	10.0.160.61	10.0.0.0/16		January 1,

TacitRed alerts underwriters to the following:

1. If a company's assigned IP space communicates with known malicious infrastructure

- TacitRed collects and refines threat intelligence on high-profile ransomware groups. Including collection of their malicious command and control infrastructure. We alert an underwriter any time a login or probe is attempted by threat actors towards any company of interest's network.

2. If a third-party vendor is at major risk of a breach that would affect a potential insured

- TacitRed monitors the third-party vendors for any given company. Many ransomware events start with an MSP or MSSP getting socially engineered to proliferate attacks against their clients. We close this blind spot by tracking third-party risk, alerting an underwriter to previously unknown aggregated risk.

3. If malware is already on the network

- TacitRed tracks command and control beacons to malicious infrastructure and intercepts stolen credentials and session stealers in real time. Credentials and session cookies are used by adversaries to get initial access to accounts that are very often the root cause of high-profile ransomware breaches. An underwriter could use this data to avoid a claim, since they would know a company is already infected.

4. If technology is in place on client networks that is known to be targeted by adversaries

- We track adversary tactics, techniques, and procedures to determine real risk. If adversaries are socially engineering to get into a specific technology, we receive this data in our threat intelligence, and notify on it. Gone are the days of third-party risk reports where findings are unconfirmed and irrelevant.

> **Due to the extreme speed at which TacitRed reports these findings, a social engineering loss in the tens of millions or more can be avoided.**
>
> **Hackers are incredibly clever. Help your underwriters make the right decisions and avoid major pitfalls.**
>
> **Give your employees a fighting chance with TacitRed.**

TacitRed