NISOS

THREAT ANALYSIS

Karakurt vs. Conti Compare and Contrast

As it pertains to cyber insurance and current OFAC sanctions

JULY 2023

RESEARCH

Table of Contents

DISCLAIMER:

The reporting contained herein from the Nisos research organization consists of analysis reflecting assessments of probability and levels of confidence and should not necessarily be construed as fact. All content is provided on an as-is basis and does not constitute professional advice, and its accuracy reflects the reliability, timeliness, authority, and relevancy of the sourcing underlying those analytic assessments.

Executive Summary

With a handful of recent cyber threat intelligence reports alleging direct organizational ties between Conti and Karakurt[1] - some may ask ***why does it matter if Karakurt is an organizational component of Conti as opposed to an ecosystem affiliate?***

Although seemingly simple, this question has significant implications for insurance providers and policyholders alike. Members of Conti are specifically identified as a Russia-aligned OFAC sanctioned entity whereas Karakurt is not, nor are any of its members. It is illegal in the United States to make any payment to Specially Designated Nationals (SDNs) identified to be Conti members[2] whereas Karakurt payments are not contraindicated directly. However, in 2022 Arctic Wolf, ChainAnalysis and Intel471 reporting hypothesized the link between Karakurt as an extension of Conti.[3][4]

Karakurt's specialty is data exfiltration and publicly posting or shaming a victim if payment is not made, making it a 'double extortion' tactic. This type of attack involving data theft as a component of the operation has increased significantly, now occurring in approximately 70% of negotiated ransomware cases, up from ~40% in mid-2021.[5] In this article we outline the implications of double extortion tactics and of the current affiliate ecosystem for insurers and insured alike.

Karakurt Group Lineage

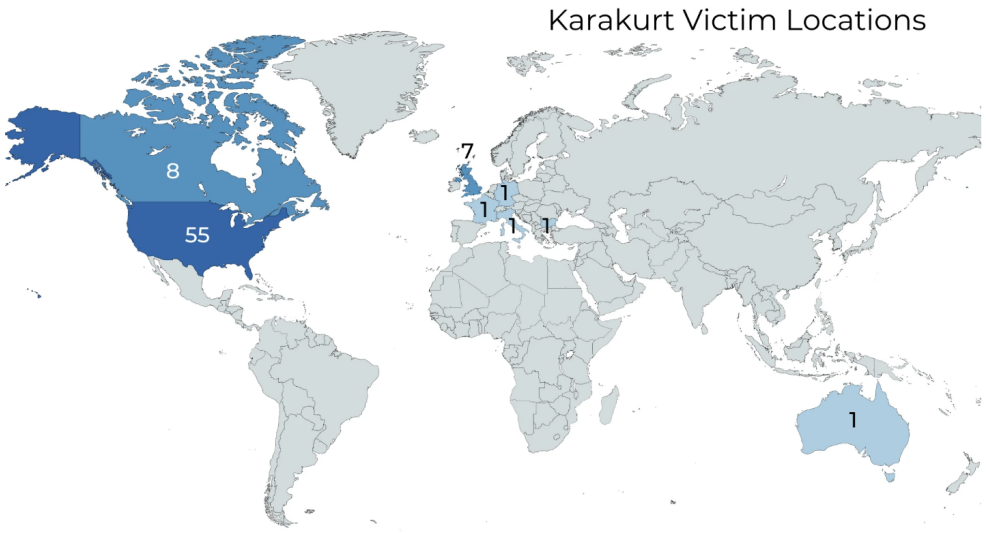
Before diving into the technical reasons for this hypothesis, let's start with a brief overview of the Karakurt group itself. The name's origin can be traced back to one of the world's most dangerous spiders known to live specifically in Russia's Astrakhan region,[6] as well as other parts of eastern Europe and Siberia.[7]

Graphic 1: Karakurt Ransomware Group Logo[8]

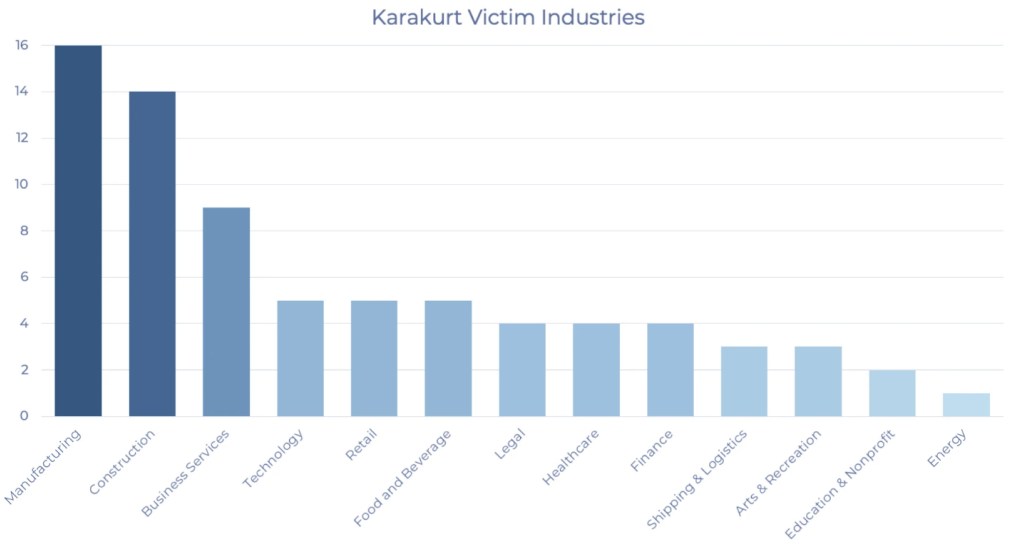
Graphic 2: Karakurt spider[9]

[1]https://www.bleepingcomputer[.]com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate
[2] https://cyberscoop[.]com/state-department-10-million-bounty-russian-intelligence/
[3] https://intel471[.]com/blog/using-cybercrime-as-cover-how-conti-operators-are-lying-low
[4] https://arcticwolf[.]com/resources/blog/karakurt-web/#_ftn1
[5]https://start.paloaltonetworks[.]com/2023-unit42-ransomware-extortion-report?utm_source=google-jg-amer-unit42&utm_medium=paid_search&utm_term=ransomware&utm_campaign=google-unit42-unit42-amer-multi-lead_gen-en&utm_content=gs-16992445439-144885984601-652945132484&sfdcid=7014u000001VVbzAAG&gad=1&gclid=CjwKCAjwhJukBhBPEiwAniIcNXuMvJpIHsOoI7dFCmxwgvn5XfeArAmO7_cZC1vkW-VB6Ys6md9t6xoCQi4QAvD_BwE
[6]https://travelsnippet[.]com/asia/russia/the-most-dangerous-animals-in-russia/#:~:text=Karakurt%20Spider,-Photo%20by%20Wikimedia&text=These%20spiders%20can%20be%20encountered,karakurt%20spiders%20is%20fairly%20easy.
[7]https://en.wikipedia.org/wiki/Latrodectus_tredecimguttatus#:~:text=In%20Kazakhstan%20%E2%80%93%20where%20it%20has,species%20biting%20and%20killing%20camels
[8]https://arcticwolf[.]com/resources/blog/karakurt-web/
[9]https://simbania.wordpress[.]com/2018/11/30/animal-of-the-day-11-30-2018-the-karakurt-spider/

First identified in June of 2021, Karakurt labels itself as a ransomware group, but its tactics, techniques, and procedures (TTPs) appear to be more focused on data exfiltration and the related secondary or double-extortion tactic of holding an organization ransom by threatening to release sensitive stolen information.[10] Quickly gaining traction, the group amassed over 40 victims across multiple market segments, 95 percent of which were in North America or Europe in the final months of 2021.[11]



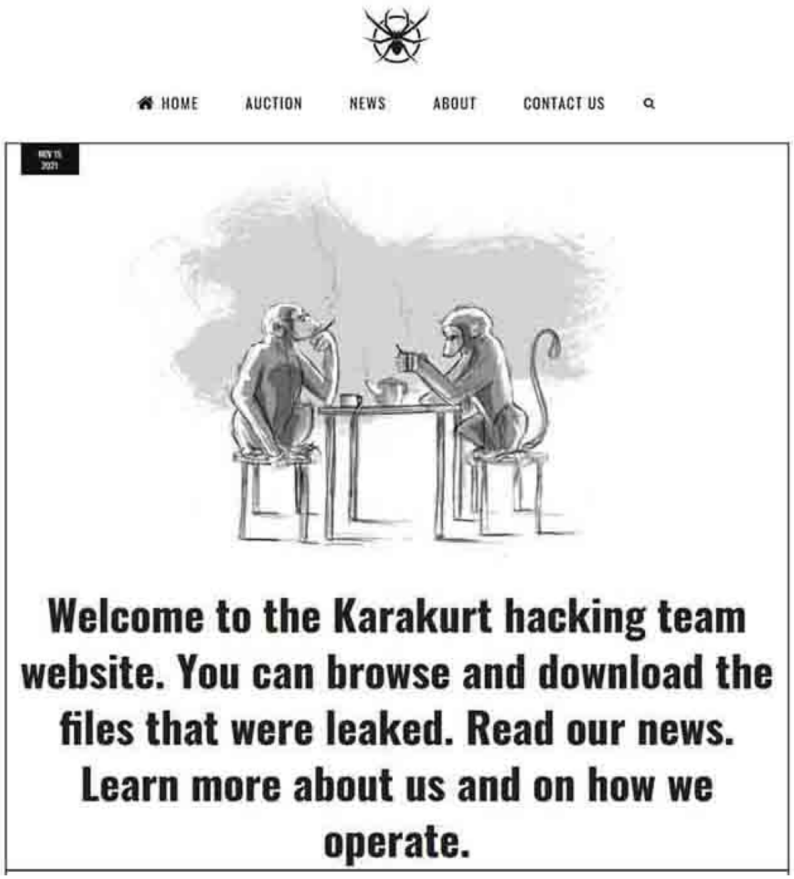
Graphic 3: Initial Karakurt non-ransom-paying victims mapped by country.[12]



Graphic 4: Initial Karakurt non-ransom-paying victims mapped by market segment.[13]

[10]https://www.accenture[.]com/us-en/blogs/cyber-defense/karakurt-threat-mitigation
[11]https://threatpost[.]com/karakurt-conti-diavol-ransomware/179317/
[12]https://arcticwolf[.]com/resources/blog/karakurt-web/#_ftn1
[13]https://arcticwolf[.]com/resources/blog/karakurt-web/#_ftn1

Both Karakurt[.]group and karakurt[.]tech were registered on June 5th, 2021, with the Twitter handle *karakurtlair* created later in August of 2021, allowing the group to reveal its first victim on karakurt[.]group on November 17th, 2021.[14] Two days later, the group updated Karakurt[.]group by adding a "News" page which hosted three volumes of their "Autumn Data Leak Digest".[15]



Graphic 5: Karakurt Group Tor Home Page[16]

As previously stated, Karakurt's specialty is data exfiltration and extortion as opposed to the more typical mass-encryption-style ransomware attacks. While specific TTPs are outlined below in the Connected Hypothesis section, it's worth noting that this group is adept at leveraging native tools and favors a "Living-off-the-land" (LotL) approach for post-exploitation as opposed to the commonly observed and typically monitored for Cobalt Strike. Karakurt targets large organizations with revenue to support higher ransom demands, typically ranging from US $25,000 to US $13 million in cryptocurrency.[17]

As a final point to consider prior to paying any ransom (as it pertains to Conti with secondary attacks attributed to Karakurt), **~80% of victims who also paid a ransom to restore systems were attacked again.[18]**

[14]https://www.accenture[.]com/us-en/blogs/cyber-defense/karakurt-threat-mitigation
[15]https://www.accenture[.]com/us-en/blogs/cyber-defense/karakurt-threat-mitigation
[16]https://arcticwolf[.]com/resources/blog/karakurt-web/
[17]https://intel471[.]com/blog/using-cybercrime-as-cover-how-conti-operators-are-lying-low
[18]https://www.newsweek[.]com/most-businesses-that-pay-off-after-ransomware-hack-hit-second-attack-study-1601266

Reasons for the *Connected Hypothesis*

The idea that Conti and Karakurt are formally connected in some capacity began when Accenture discovered a Conti-planted-backdoor being leveraged for a secondary attack by Karakurt.[19] This initial observation was further strengthened by Arctic Wolf's Tetra Defense group hypothesis that such access could only have been gained via some type of organized purchase, pre-established operational relationship, or by some type of Karakurt compromise of pre-established Conti infrastructure.[20] An additional point of similar behavior came in the form of a leave-behind file labeled "file-tree.txt" in the victim's environment, as well as the initial points of intrusion (including the use of Fortinet SSL VPNs).[21] The last nail in the proverbial coffin came when Chainanalysis identified dozens of cryptocurrency wallets belonging to Karakurt that were transferring significant funds to Conti-owned wallets. In the same analysis, security researchers also discovered a shared wallet hosting both Conti and Karakurt victim payment addresses leaving little doubt that both were deployed by the same affiliate.[22]

Compounding Ecosystem, Environmental & Threat-Related Variables

Cybercrime is not slowing down, but rather the industry as a whole is expected to grow to over $265 billion by 2031.[23] The same source revealed early 2023 statistics supporting 62% of attacks spanning four continents, and over 10 market segments were focused in the domestic United States.[24] This statistic is also supported by the heatmap provided by the 2021 Ransomware Task Force (made up of Palo Alto Networks Unit 42, Cloudian, Black Fog, Recorded Future and others) where ~60% or ~2000+ out of a globally observed total of ~3340+ incidents targeted the domestic US.[25]

Multi-extortion tactics are also on the rise as criminal operators realize that applying various forms of pressure increases the odds of ransom payment. In late 2022, Palo Alto Networks' Unit 42 noted ~70% of cases involved data theft in addition to the primary encryption event; up from ~40% in mid 2021.[26] Another payment pressure trend on the rise is the concurrent harassment of either customers or business partners, and/or engaging the media. This metric rose from less than 1% in mid 2021 to ~20% by late 2022.[27]

[19]https://www.accenture[.]com/us-en/blogs/cyber-defense/karakurt-threat-mitigation

[20]https://arcticwolf[.]com/resources/blog/karakurt-web/

[21]https://threatpost[.]com/karakurt-conti-diavol-ransomware/179317/

[22]https://threatpost[.]com/karakurt-conti-diavol-ransomware/179317/

[23]https://flashpoint[.]io/blog/guide-to-ransomware/

[24]https://flashpoint[.]io/blog/guide-to-ransomware/

[25]https://securityandtechnology[.]org/blog/rtf-year-two-new-map-new-data-same-mission/

[26]https://start.paloaltonetworks[.]com/2023-unit42-ransomware-extortion-report?utm_source=google-jg-amer-unit42&utm_medium=paid_search&utm_term=palo%20alto%20ransomware&utm_campaign=google-unit42-unit42-amer-multi-lead_gen-en&utm_content=gs-16992445562-135418591083-652945132496&sfdcid=7014u000001VVbzAAG&gad=1&gclid=Cj0KCQjw1rqkBhCTARIsAAHz7K36bGm1DiHRoFR1qaWNK0vBTAQvN-ddHXpN5gPjQXlDlujuhbaBlVkaAjnnEALw_wcB

[27]https://start.paloaltonetworks[.]com/2023-unit42-ransomware-extortion-report?utm_source=google-jg-amer-unit42&utm_medium=paid_search&utm_term=palo%20alto%20ransomware&utm_campaign=google-unit42-unit42-amer-multi-lead_gen-en&utm_content=gs-16992445562-135418591083-652945132496&sfdcid=7014u000001VVbzAAG&gad=1&gclid=Cj0KCQjw1rqkBhCTARIsAAHz7K36bGm1DiHRoFR1qaWNK0vBTAQvN-ddHXpN5gPjQXlDlujuhbaBlVkaAjnnEALw_wcB

With Ransomware-as-a-Service (RaaS), the evolving ecosystem is divided among actual RaaS Syndicates, Initial Access Brokers (IABs), other support operators, and the actual do-ers who are typically referred to as Affiliates. The RaaS model lowers the barrier to entry for less skillful attackers, and tokenizing these illicit services results in operators procuring new combinations of services for each campaign or sometimes each operation. This model is discussed in greater detail in our prior article[28] and presents significant new challenges in terms of threat actor attribution.[29]

Where current Office of Foreign Assets Control (OFAC) sanctions are associated with either *SDNs or specific entities*, threat actor attribution is becoming more critical while the evolving criminal ecosystem is making attribution even more complex. Attacks often involve stringing together the services of multiple providers and therefore direct attribution to a specific group becomes more challenging. Further compounding the situation are multiple recent nation state toolkit leaks,[30] prolific vulnerabilities to exploit like Log4J,[31] the Conti breakup,[32] events like the Lockbit3.0 source code disclosure,[33] as well as a proliferation of one-off groups (sometimes to shift law enforcement focus off primary groups). In this same timeframe blue-teamers have witnessed a tactical evolution in the form of many attackers pivoting to using existing tools from the victim's environment, making any specific unique signature hard to come by (commonly referenced LotL attacks).

When ransomware or the related double extortion events occur, attackers typically expect payment within the first two weeks–with contact expected in the first 72 hours–or there is normally a penalty imposed. The average negotiation window has been expanding since 2020 when it was approximately five days, then approximately eight days in 2021, and so on.[34] It is encouraging that the negotiation window is expanding along with the reduced percentage of ransomware payers over the same window; 76% paying ransoms in 2019, 50% in 2020, and 41% in 2022.[35] Industry leaders cite this trend as continuing into the first half of 2023 with only 25-30% of victims recovering or suppressing public release via ransom payment.[36]

During this critical window of time, several primary activities need to occur within a victim organization:

> #1: The organization needs to confirm scope of impact, communicate as necessary, and determine if internal recovery is possible. Mitigation recommendations specific to Karakurt can be found in the June 2022 CISA Cybersecurity Advisory (Alert Code: AA22-152A).[37]

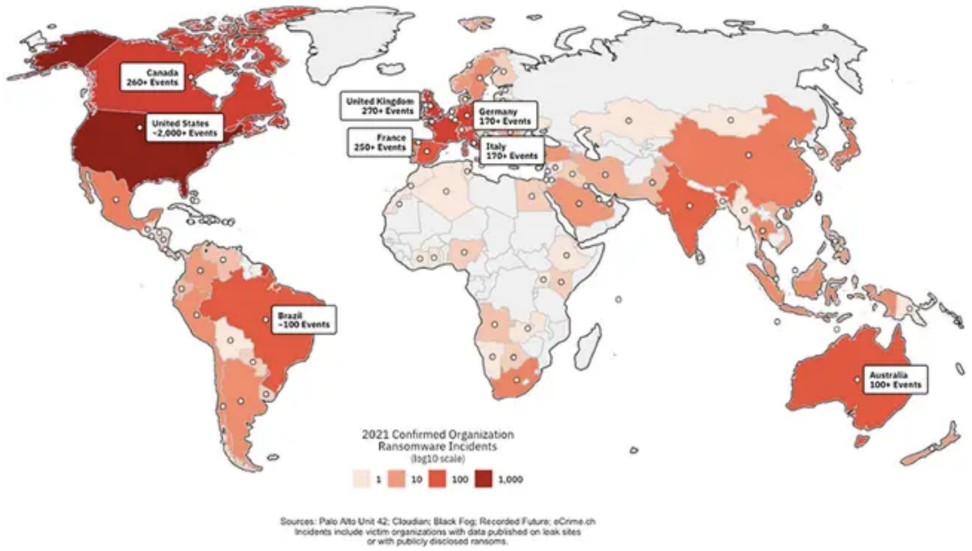
[28]https://www.linkedin[.]com/pulse/ransomware-as-a-service-raas-where-do-we-from-here-m-mba-itil-?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
[29]https://www.linkedin[.]com/pulse/ransomware-as-a-service-raas-where-do-we-from-here-m-mba-itil-?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
[30]https://arstechnica[.]com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/
[31]https://theconversation[.]com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896
[32]https://thehackernews[.]com/2022/05/conti-ransomware-gang-shut-down-after.html
[33]https://intel471[.]com/blog/lockbit-3-0-builder-code-leak-points-to-another-disgruntled-criminal-employee
[34]https://www.scmagazine[.]com/analysis/ransomware/ransomware-negotiations-are-taking-longer-and-thats-a-good-thing
[35]https://www.darkreading[.]com/attacks-breaches/ransomware-profits-decline-victims-refuse-pay
[36]https://www.csoonline[.]com/article/3607689/how-ransomware-negotiations-work.html
[37]https://www.cisa[.]gov/news-events/cybersecurity-advisories/aa22-152a

#2: The organization needs to engage the threat actor if for no other reason than to string them along and provide more time for internal recovery efforts. However, more often than not critical intelligence can be gained in this window of time. The victim organization can look to attribute the specific threat actor if not already known and confirm if they are an OFAC-sanctioned entity, as well determine if there is any data on prior engagements with the group (i.e. how often decryption is successful or how often public disclosure occurs).

#3. The organization should engage its legal counsel and use a third party investigative firm to ensure that its coordination efforts are in lockstep and satisfy the legal requirements of all stakeholders. These experts can also gauge the applicability of law enforcement involvement, and can apply attorney-client privilege to any related communications or reporting to assist legal counsel with any downstream litigation. This group can also provide a legal perspective on any planned remediation or mitigation tactics.

According to BakerHostetler, those paying over $1M typically pay in eight days whereas 10 days is normal for those organizations paying between $200K and $1M.[38] Based on this timeline, a victim organization likely has 8-14 days before payment needs to occur for decryption-key-based-recovery or internal recovery must prove successful. Additionally, if data was exfiltrated the victim organization has to determine if the threat actors publicly shame delinquent or non-paying victims. This does not give a victim organization much time to potentially bring in external counsel and additional technical resources, much less confirm if the threat actors involved are subject to OFAC or any specific terms of their cyber insurance coverage.

Although ransomware is a global issue, it is a US domestic epidemic. Over 60% of the attacks are focused on US victims according to Flashpoint in their April 2023 Ransomware Overview.



Graphic 5: Heatmap of 2021 ransomware attacks[39]

[38]https://www.bakerlaw[.]com/BakerHostetler-Launches-2022-Data-Security-Incident-Response-Report-Resilience-and-Perseverance

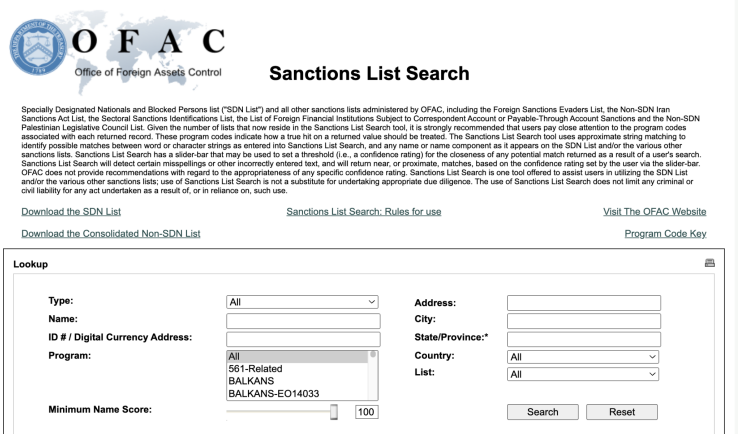
[39]https://securityandtechnology[.]org/blog/rtf-year-two-new-map-new-data-same-mission/

Graphic 6: Flashpoint Ransomware Overview - April 2023[40]

Office of Foreign Assets Control (OFAC) Cyber Sanctions Overview and Challenges

According to the U.S. Treasury Department, SDNs can be "front companies, parastatal entities, or individuals determined to be owned or controlled by, or acting for or on behalf of, targeted countries or groups. They also can be specially identified individuals such as terrorists or narcotics traffickers. SDNs are designated primarily under the statutory authority of the Trading With the Enemy Act, the International Emergency Economic Powers Act, the Anti-Terrorism and Effective Death Penalty Act, and the Foreign Narcotics Kingpin Designation Act."[41]

The current system has a web-facing interface where users can query whether or not an SDN, as defined by the US Treasury Department, has a sanction against them. Searching can be difficult and it is highly recommended for organizations to seek qualified help when attempting to confirm if the entity they are interacting with is potentially under OFAC sanctions.



Graphic 7: OFAC Sanction List Search Homepage[42]

[40]https://flashpoint[.]io/blog/cyber-threat-intelligence-index-may-2023
[41]http://www.treas[.]gov/offices/enforcement/ofac/
[42]https://sanctionssearch.ofac.treas[.]gov/

Beyond the complexity of searching, there is the more pressing policy-level challenge of how to address more ephemeral associations or relationships between threat actors. Consider for a second that we have two bad guys, bad guy A (BGA) is sanctioned under OFAC whereas bad guy B (BGB) is not. Suppose at one point BGA attacked our hypothetical company, ACME corporation. Later BGA sold ACME corporation network access to BGB who executed a secondary attack on ACME. In this scenario or one where shared infrastructure is leveraged for some part of a secondary attack, or some portion of crypto funds are routed to the digital wallet associated with a OFAC-sanctioned party - is the whole attack then de facto subject to OFAC sanctions? Currently the only related language is outlined in the Department of Treasury's Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments dated September 21, 2021.[43]

Impact to Insurers and the Insured

Insurance decisions are centered around accurately quantifying risk and charging an appropriate premium to statistically cover any downstream payouts. With a highly dynamic or fluid threat environment, governments around the world are taking actions against cyber threat actors in the form of regulations or sanctions. Insurance providers are incorporating these new developments in new ways in an ongoing effort of minimizing their portfolio risk exposure. This has manifested in even more nuanced policy terms and conditions, as well as situations where coverage is not extended due to the perceived threat actor attribution and some associated sanction.

Simultaneously the insured are working through the challenge of getting cyber insurance with the expectation that when they have a significant event this policy/coverage will come to their aid. The sobering reality of the March 31st, 2023 war clause decision by Lloyd's of London[44][45] makes attack-related-losses from events like NotPetya in 2017 non-recoverable.[46] At the same time other Insurers are offering broad or blanket coverage policies like the $45M cyber catastrophe fund offered by Beasley.[47]

The reality of the current situation is claimants are being met with Insurer push-back based on perceived threat actor affiliations. In the US, cases are being waged currently to determine if different parts of the affiliate ecosystem should be considered part of the same criminal organization or not. The merits of those cases will set precedents going forward in terms of situations like Conti and Karakurt where the services the two groups provide mesh well in terms of operational effectiveness.

Cyber-borne lawsuit trends in general (inclusive of those related to companies that collect data and/or manage the digital assets of other entities) are becoming a more regular occurrence with active litigation currently related to the "California Invasion of Privacy Act, the Video Privacy Protection Act, Right of Publicity Statutes, the Illinois Biometric Information Privacy Act and the Health Insurance Portability and Accountability Act, as well as a wave of litigation based on website tracking technology."[48]

In order to prevent this situation from getting uglier, we have two primary challenges:

[43]https://ofac.treasury[.]gov/media/912981/download?inline
[44]https://www.cpomagazine[.]com/cyber-security/lloyds-of-london-nation-state-attacks-no-longer-a-part-of-cyber-insurance-coverage-as-of-2023/
[45]https://techmonitor[.]ai/technology/cybersecurity/lloyds-of-london-cyber-war-exemption-rules-effect-today
[46]https://www.zdnet[.]com/article/notpetya-an-act-of-war-cyber-insurance-firm-taken-to-task-for-refusing-to-pay-out/
[47]https://gizmodo[.]com/insurance-cyber-catastrophe-bond-beazley-cybersecurity-1849965561
[48]https://www.google[.]com/url?q=https://www.bakerlaw.com/press/bakerhostetler-launches-2023-data-security-incident-response-report&sa=D&source=docs&ust=1687261546922533&usg=AOvVaw2FiZoSw8FQRl3ffTyWAHzN

- *Internal assessment of security controls needs to improve:* The whole industry has to get better at cyber risk quantification. Gone are the days where an insurance or third party security questionnaire can accurately gauge the effectiveness of implemented security controls by asking questions like "Does the organization have EDR deployed within the environment?" Organizations that answer 'yes' are not necessarily being asked to demonstrate full compliance. For example, *the reality may be that EDR is rolled out in the lab environment and currently deployed to five non-production machines as opposed to having the thousands in production covered.*
- *Organization-specific threat modeling capabilities need to be improved/standardized:* In today's time of constrained resources, organization's must have better business-educated cyber components. The organization's core objectives need to be well understood and the supporting systems need to be mapped and prioritized in terms of resiliency goals. On the human side, employee risk profiling (ie. VIPs, Money Movers, 3rd Party Interacters, Sys Admins, Sensitive IP Handlers, Developers) needs to be incorporated as the vast majority of attacks start with some form of social engineering and there is a growing risk of insider threat. This is the bedrock prerequisite to being able to perform holistic cyber risk quantification along with understanding what is most important to the business and what digital assets support those outcomes.

How does all this translate to premiums and coverage reductions? From a study released in May 2023 in which 450 IT and Cyber decision makers were polled, 74% noted increased premiums, 43% cited increased deductibles and 10% saw a reduction in coverage benefits.[49]

Looking forward, more cyber insurance providers are stepping into the ring which is helping both build additional coverage capacity industry-wide as well as diluting the year-over-year rate increases. Even with this additional capacity and the 30-50% rate increases from 2022 behind us, increases are still forecasted for 2023 albeit at a much slower rate (projected in the 5-10% range).[50]

Conclusion: Re-evaluating the *War Exclusion Clause* in our current Dynamic Threat Environment

Lloyd of London's cyber war exclusion clause may have just recently taken effect on March 31, 2023, but the final coverage implications of that decision are far from determined. In early May 2023, a New Jersey appellate court ruled $1.4B in Merck's favor that a group of insurers would not be able to leverage the war clause exclusion as a means to not pay Merck for losses related to the 2017 NotPetya attack.[51] This decision clearly shows cyber risk quantification as less mature than required by industry where insurance providers are looking for means of limiting exposure while the insured are forced into litigation in order to receive post-loss cyber insurance funds.

This should be a stark warning for all small to medium enterprises that do not have the legal budget to engage in prolonged litigation in order to finally receive remuneration for losses that were already

[49]https://www.securitymagazine[.]com/articles/99390-ransomware-is-being-excluded-from-cyber-insurance-policies
[50]https://www.insurancejournal[.]com/news/national/2023/01/30/705209.htm
[51]https://www.fiercepharma[.]com/pharma/merck-entitled-14b-payout-cyberattack-case-after-judge-refutes-insurers-warlike-action-claim

incurred. The war clause exclusion has dramatically and negatively impacted the beneficiaries of cyber insurance and made any type of cyber risk transference much more challenging. As a result, cyber insurance premiums continue to rise, coverage reductions are forcing the need for threat actor attribution if for no other reason to support breach follow-on litigation. Just as attribution is becoming more important, having an organization-specific risk understanding married with a current adversary threat perspective is critical in order to accurately quantify cyber risk.

Appendix A: OFAC-related Executive Orders, Regulations, and Statutes

These authorities are further codified by OFAC in its regulations which are published in the Code of Federal Regulations (CFR). Modifications to these regulations are posted in the Federal Register. [52][53]

Executive Orders

- 13757 - Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities (December 28, 2016)
- 13694 - Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (April 1, 2015)

Statutes

- Information on Countering America's Adversaries Through Sanctions Act
- International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-1706
- National Emergencies Act (NEA), 50 U.S.C. §§ 1601-1651

Code of Federal Regulations

- 31 CFR Part 578 - Cyber-Related Sanctions Regulations

Federal Register Notices

- 87 FR 78484-22 - Publication of Humanitarian Sanctions Regulations Amendment and General Licenses (Nongovernmental Organizations, Agricultural, and Medicine)
- 87 FR 54373-22 - Cyber-Related Sanctions Regulations
- 80 FR 81752-15 - Issuance of Cyber-Related Sanctions Regulations to implement Executive Order 13694

[52] http://www.treas[.]gov/offices/enforcement/ofac
[53] https://tradecomplianceinstitute[.]org/p_show_faq_answers.php?id=220