Analyzing the extortion note of BlackCat/ALPHV - hacking to the systems of the Israeli fintech company "Tipalti" 3.12.23.

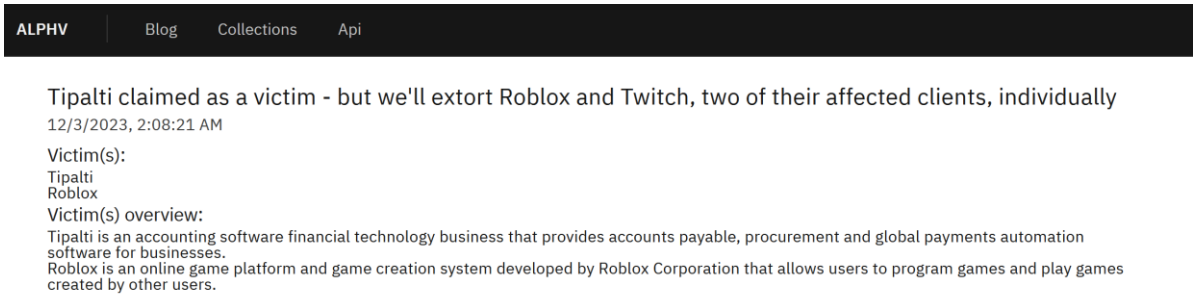

Figure 1 - the logo of one of the victim organisations, Roblox

Figure 2 – the logo of one of the victim organisations, Tipalti

Insights summary:

ALPHV blackmail note is a bit extraordinary, in its creativeness, in its intention to blackmail only “Tipalti” customers, in its attempt to damage “Tipalti” reputation and to create collateral damage to “Tipalti” clients. In addition to extort money ALPHV seems eager to harm “Tipalti” reputation.

Here is a breakdown of the insights:

- ALPHV intends to blackmail only “Tipalti” customers.
- According to ALPHV, the company "Tipalti" cannot afford to pay, unlike wealthy Roblox.
- It is possible that the ransom group only has access to several customers' accounts and not to the entire "Tipalti" system.
- ALPHV group does not mention data encryption, only customers' data that will be leaked.
- ALPHV threatened that as soon as the stock market opens tomorrow, Monday, they will leak more information about the clients.
- ALPHV claim that an inside employee assisted them.
- They leak only “Tipalti” customers' data because they believe that management is incapable of handling the incident and know that “Tipalti” insurance doesn't cover cyber incidents.
- ALPHV know that Roblox was extorted by another group last year and did not pay the ransom.
- ALPHV threatens to leak sensitive information of “Tipalti” customers, for months
- ALPHV continues with a specific threat on Roblox. They intend to leak sensitive information about Roblox creators.
- From the moment the sensitive information samples are sent, the ransom group gives Roblox two hours to negotiate or leak information.

(C)All rights reserved to ClearSky Cyber Security Ltd. 2023 info@clearskysec.com
www.clearskysec.com

The following notification was published on the ALPHV website.

Blackmail message	Insights
Tipalti claimed as a victim - but we'll extort Roblox and Twitch, two of their affected clients, individually	ALPHV intend to extort only "Tipalti" customers.
Context *We have remained present, undetected, in multiple Tipali systems since September 8th 2023.*	It is possible that the ransom group only has access to several customers' accounts and not to the entire "Tipalti" system.
Over 265GB+ of confidential business data belonging to the company, as well as its employees and clients has been exfiltrated.	ALPHV group does not mention data encryption, only customers' data that will be leaked.
*We remain committed to this **exfiltration operation**, so we plan to reach out to both these companies once the market opens on Monday as we believe we will have an even greater amount of data by then,*	ALPHV threatened that as soon as the stock exchange opens tomorrow, Monday, they will leak more sensitive information of "Tipalti" clients.
in addition to the likely inability of the Tipali company to be able to contain our efforts by then, given their incompetency and taking into account **that an insider was , and is still actively involved**.	ALPHV claim that an inside employee in "Tipalti" assisted them.
*This article will be republished on Monday just before the market opens, **to maximize the impact to the $RBLX stock price.***	Again, they threaten to impact "Tipalti" clients shares
*Outing victims before they even get a chance to respond is a bad business practice, but given that **Tipalti's insurance policy does not cover cyber extortion** and considering the behavior of the executive team in general, observed through internal communications, we believe the likelihood of them reaching out on our terms is unlikely, regardless of the sensitivity of data in question.*	They leak only "Tipalti" customers' data because they believe that "Tipalti" management is incapable of handling the incident and know that Tipalti insurance doesn't cover cyber incidents.
*Another justification for this outing is due to us identifying a previous extortion attempt that occurred **last year by a different group** where the Roblox company engaged in excessive stalling, over a considerable period of time - **we observed that no payment was made** in this case.*	ALPHV know that Roblox was extorted by another group last year and did not pay the ransom.
*We will treat potential smart-asses like the filthy criminals they are**. If these 2 victims do not pay up, we will engage in the publication of data in multiple phases**, over the next few months, to maximise the impact to the companies and affected clients.*	ALPHV threatens to leak "Tipalti" customers sensitive information for months.

(C)All rights reserved to ClearSky Cyber Security Ltd. 2023

Blackmail message	Insights
*In the case of Roblox, we plan **to individually extort affected parties such as their creators**, for who we have significant confidential for, including tax documents.*	ALPHV continues with a specific threat on Roblox. They intend to leak sensitive information about Roblox creators.
*If you are not prepared to talk figures within **2 hours** of receiving the file lists or samples, we will immediately resort to the strategies we have mentioned earlier. There is no room to negotiate for these 2 companies, you either pay or you don't.*	From the moment the sensitive information samples are sent, the ransom group gives Roblox two hours to negotiate or leak information.
To conclude… according to scholarly articles in this field such as the work of Dykstra et al. (2022), paying a ransom has possible benefits, such as in situations where the impacted organization faces significant negative externalities, which these victims do.	Pure poetry
We look forward to reaching a resolution here. ***References list*** *Dykstra, Josiah, et al. "Opportunity cost of action bias in cybersecurity incident response". Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 66, no. 1, 2022, p. 1116-1120. https://doi[.]org/10.1177/1071181322661490*	Pure poetry

(C)All rights reserved to ClearSky Cyber Security Ltd. 2023 info@clearskysec.com
www.clearskysec.com