Conti Ransomware | Arctic Wolf

arcticwolf.com/resources/blog/conti-ransomware-leak-analyzed

March 16, 2022

Conti Ransomware: An Analysis of Key Findings

Key Takeaways

- Internal chats between individuals of the Conti ransomware group further reveals the structure of their Ransomware as a Service (RaaS) model.
- Overwhelmingly, Conti's victims have been based in the US, followed by Germany.
- Certain individuals within the Conti ransomware group fulfill financial, technical, and management responsibilities as opposed to fully automated solutions.
- Chats occur between 442 individuals, 44 of which are considered to be "core" members of the Conti ransomware group.
- Political affiliations between individuals of the Conti ransomware group are not homogenous, and in fact, can be contentious.

Conti Ransomware. New Conflict, New Information

Amidst the turmoil of the Ukraine-Russia conflict, incident responders and ransomware researchers observed several ransomware gangs publish statements on their dark web blog sites. Some actors asserted the apolitical nature of their operations, while others clearly favored a side.

Most notably, the Conti ransomware group posted a public statement in support of Russia with a stern warning of retaliation on February 25, 2022. Shortly after this, cyber defenders quickly learned that Conti's pro-Russian support was not representative of the group's

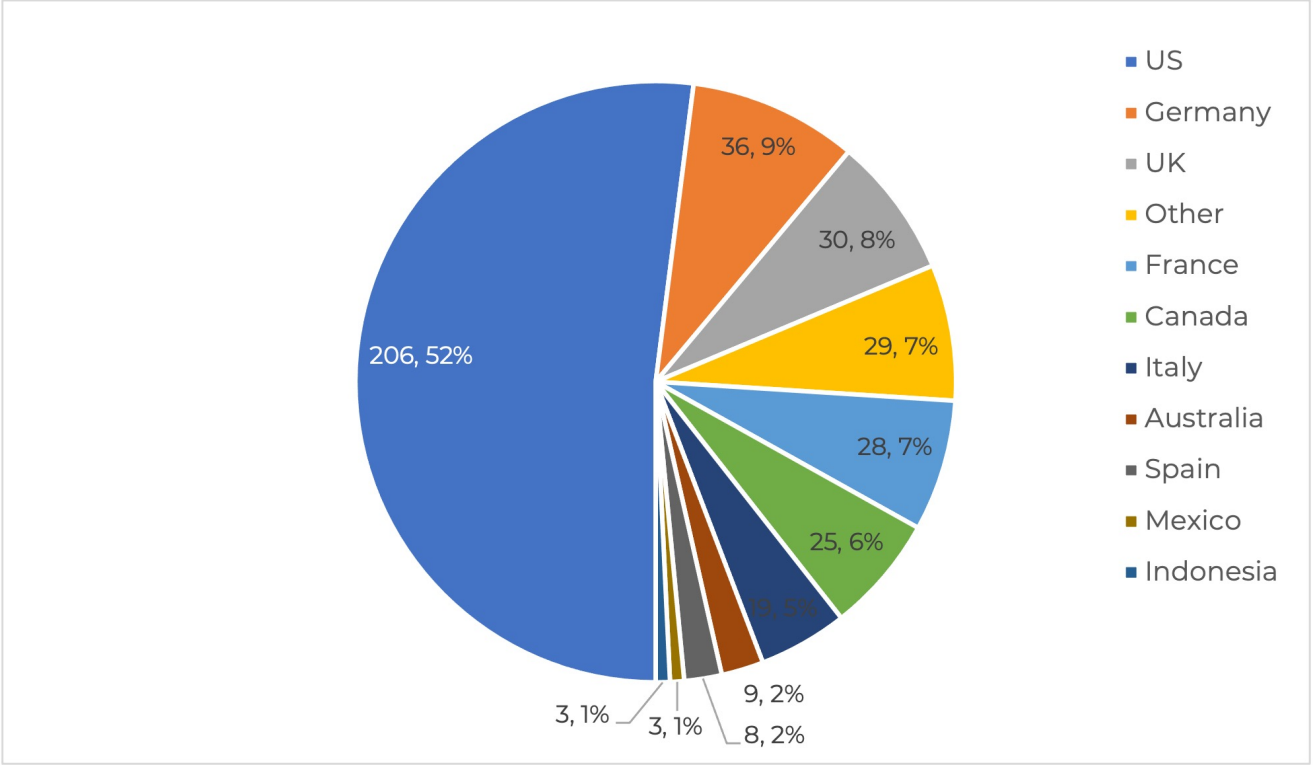
constituents. In an ironic turn of events, after Conti exposed private data from extorted companies over the past year and a half, Conti's *own* sensitive data has now been exposed.

Going by the handle "@ContiLeaks" on Twitter, individual(s) with access to internal Conti data began publishing large archives of information, including Conti's internal chats from Jabber, details on infrastructure, internal documents, and even source code stating emphatically, "Glory to Ukraine." While third-party leaks cannot be fully verified, many of their contents correspond to Conti's dark web posts and our direct experience with this threat actor. Our analysis can shed light on the nature of communications between the alleged individuals operating within the Conti threat actor group.

Conti Victim Demographics

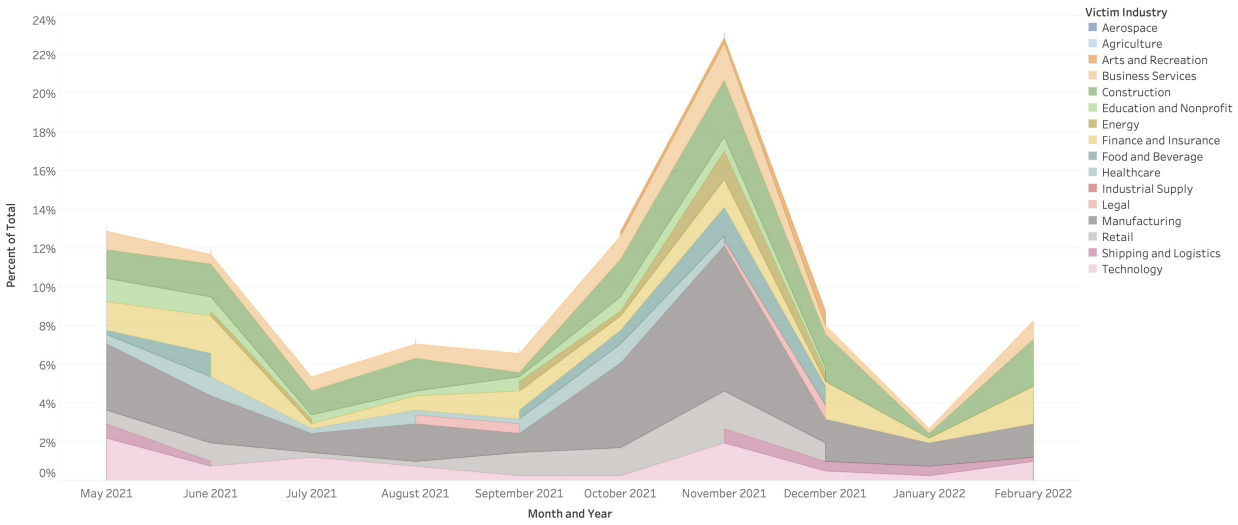
For background, Conti is one of the most prolific ransomware groups that we have tracked over the past 21 months, often ranking in the top 5 of 'most posted victims' on their dark web site, where victims who don't pay up, are exposed and shamed. From monitoring their dark web posting activity to responding to ransomware attacks initiated against businesses in real-time, we can use our own data to contextualize this latest leak.

Conti Dark Web Victims by Geographic Location



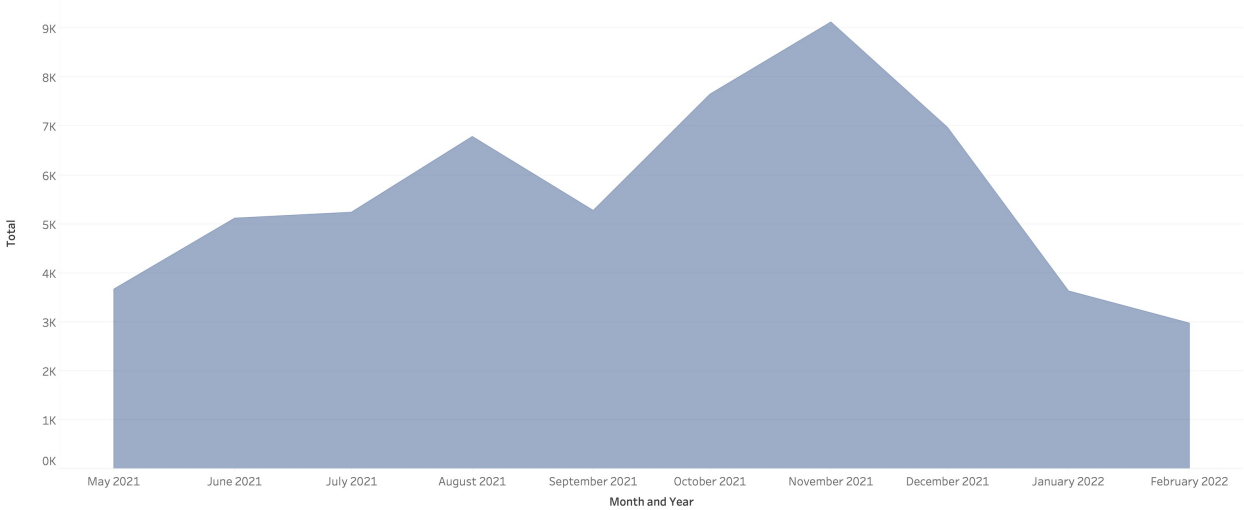
Overwhelmingly, Conti's claimed ransomware victims are headquartered in the United States.

Conti Dark Web Claimed Victims by Industry



While victim organizations are varied, Conti's dark web blog exposed manufacturing, construction, and technology firms most often. This is not to say that firms among these industries are the most frequently targeted by the Conti group — exposure is a consequence of failed negotiations, while companies who quickly pay the ransom typically aren't exposed. Specific targeting of organizations is not the most lucrative tactic for most threat actors; their most effective strategy finds victims through automatic scanning of any vulnerabilities on the public internet that they know how to exploit, that ultimately lead to an internal network.

Conti Jabber Messages by Month



A potential pattern emerges between Conti's dark web posting activity and internal chat logs

Methodology

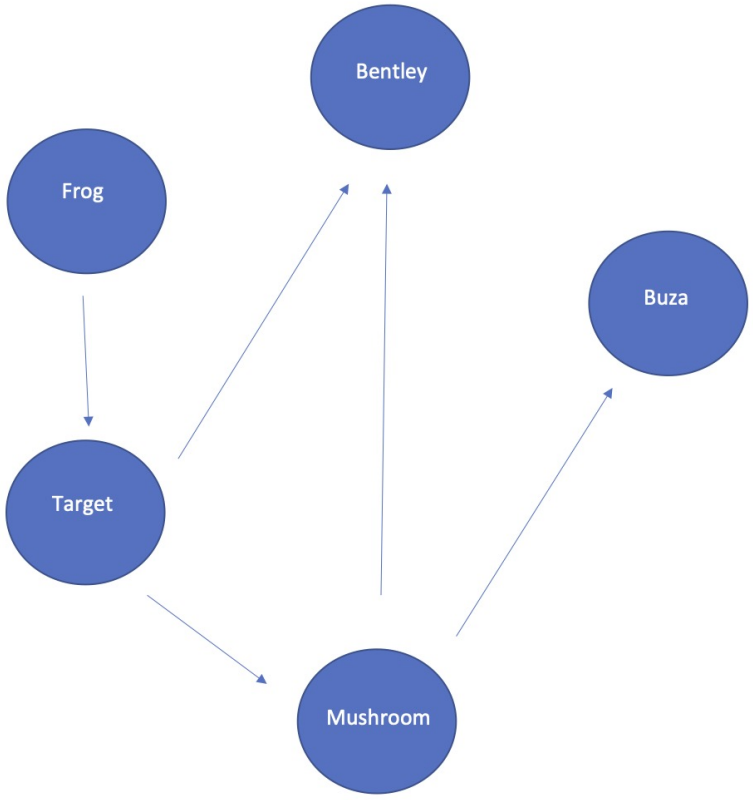
After helping victims recover from Conti ransomware incidents and tracking the group's activity for 21 months, we have become familiar with the group's tactics, techniques, and procedures (TTPs). Backed by our previous observations of the group, we can now learn more about the internal sociological makeup of the Conti gang through an analysis of the revealed chat logs, allowing us to gain an even deeper understanding of how this adversary model operates.

By providing insight into the operations of Conti, we can form a clearer picture of the threat actors behind the ransomware. By identifying who the various members are talking to, the frequency and cadence with which they communicate, and the organizational structure of the organization, we further our understanding of how to defend against one of the most prolific ransomware groups in the market. In order to dig into these areas, our methodology includes relevant chats for context and validation.

As an example of our methodology, take the following message from the leaked chat logs. On September 24, 2020, an individual going by the cryptonym *Mushroom* sent a message to another individual named *Buza* (cryptonyms have been italicized):

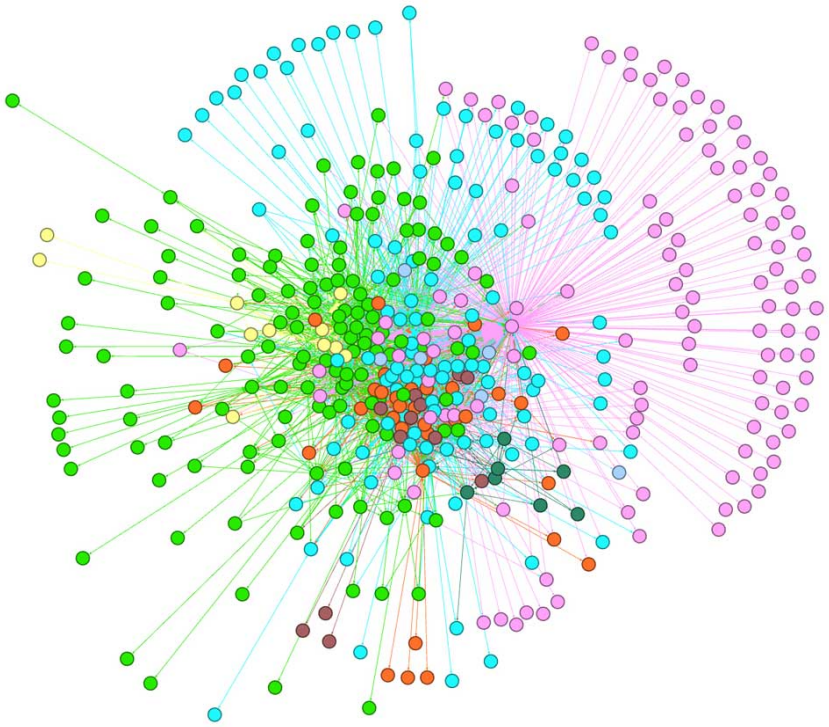
> "hello. At this point I made the bootloader for *Target* like he said, tested them, and I gave them to *Bentley*. *Frog* told him to give *Bentley* the stable version of his Bentley kit as well..."

There is considerable information in this single partial message. Focusing on the individuals and their interactions, we can think of these as a network, conceptualizing the individuals as vertices and impute edges given their reported interactions. Further, we can determine the source and target of these interactions.[1]



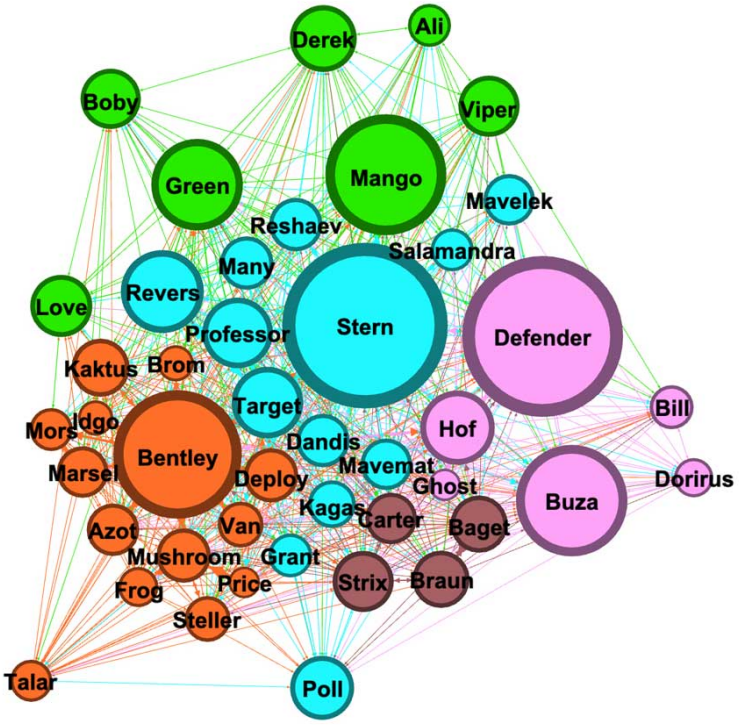
In the message, *Mushroom* provides a report to *Buza*, creating a directed edge between the two. Within the chat, we learn that *Mushroom* was tasked by *Target* to provide a deliverable to *Bentley. Target* also receives a request from *Frog* to provide a deliverable to *Bentley*. Based even on this single message, we observe a structure begin to emerge.

The interactions contained in this single chat transcript can be derived from the body of the message, and these same structures are likewise captured in the individuals' own messages to and from each other. To visualize these sender and receiver relationships, we analyzed the leaked chat data and visualized a network that yielded 442 unique chat handles, represented here as nodes.



Colored nodes indicate each detected subgroup within the Conti organization

Within the 442 nodes of the chat network, there were roughly 8 clusters or “communities” based on a community-detection algorithm. This is designed to cluster more dense connections within a subgroup and draw a boundary. This graph reflects the entire leak, with many weakly-connected nodes, so we filtered the Conti network further down to its primary members which yielded a smaller graph of roughly 44 nodes.



Still denoted by the colors of their network "communities," and labeled with their chat handles, these individuals represent the core of the Conti network graph. From here, we can begin to tease out the structure further by asking, "Who is important in this graph?"

To determine importance, we used a quantitative measure called "degree" which is simply the number of connections to other nodes. In-degree refers to the number of inbound connections (received) and out-degree refers to the outbound connections (sent). As a measure of importance, in-degree is larger for the individuals *Stern*, followed by *Defender, Bentley, Mango, and Buza.*

Name	In-Degree	Authority	Hub	PageRank	Betweenness Centrality
Stern	157	0.235122	0.308495	0.077951	0.158787
Defender	152	0.224893	0.337484	0.054485	0.286215
Bentley	118	0.214211	0.229546	0.065222	0.048557
Mango	110	0.178626	0.225409	0.026697[4]	0.060916
Buza	100	0.18	0.227305	0.016221[5]	0.053068

In-degree measures the number of individuals that communicate with the named key players. Another measure of importance is called “authority."[6] This algorithm measures not just connectedness by frequency, but the weight of importance from those connections. This can indicate a node’s authoritativeness in a network if other focal nodes point to another as a final word, destination, or “authority.”

A hub score is assigned to nodes which more reliably point to others high in authority. Like the guiding aim of authority, PageRank is a procedure designed to rank the importance of a node based on the importance of the nodes which point to it.[7]

The final algorithm used in our analysis determines “betweenness centrality,” measuring which node falls along the shortest path between any given two nodes. Being high in betweenness centrality is often a strategic position — someone who is likely a broker or gatekeeper. On this measure of betweenness, *Defender* is the most central, connecting disparate ends of the network to greater extent than any other node in the network.

Findings

Based on the analysis of the recently leaked Conti chats, it is clear that Conti’s internal structure is anything but flat and egalitarian. On all measures of centrality aside from PageRank, the same five individuals remained the most important nodes. Certain individuals hold central roles within Conti’s ransomware business structure and the various metrics of network centrality allow us to triangulate key players and positions:

Name	Position	Function
Stern	*Leader*	*Oversees the whole operation.*
Defender	*Technical Administrator*	*Manages internal infrastructure.*
Bentley	*Developer/R&D Lead*	*Oversees “cryptors” and tool obfuscation (testing against Anti-Virus solutions).*
Mango	*General Team Manager*	*Oversees personnel and manages projects, assists with payroll.*
Buza	*Coder Lead*	*Oversees teams of coders*

Stern appears to be the superior within the identified core group. It might seem puzzling, for instance, that *Stern* ranked highest in in-degree, authority, and PageRank, yet *Defender* holds advantage in betweenness centrality. This is instructive as various metrics of

importance in the network capture qualitatively different things. In examining *Defender's* network, it appears *Defender's* position resembles something of a technical coordinator for the network of Conti operatives, maintaining some of the Conti infrastructure, technical operations, and reminding new members to submit backup contacts.

Defender appears to report to *Stern*, who based on the quantitative findings, had the highest in-degree, PageRank, and authority scores. These measures can also be corroborated with qualitative analysis of messages between *Defender* and *Stern*. *Defender* provides reports upon request and was even seen calling in sick to *Stern*.

Mango, also a central node, appears to have some authority over some personnel aspects of the organization, having some involvement with hiring and payroll. Writing to Stern about the shortcomings of a lower manager after a promotion, *Mango* states,

> "*love slow down with the promotion, he's relaxed, he says he's doing a lot, but in fact there are more words than deeds and then see for yourself... I told him off, let him sweat for another month, motivated him*."

Stern, for his part instructs *Mango* to keep the other team members "*in check.*"

Mango's involvement in payroll is seen in reminding *Stern* repeatedly, "*don't forget about the paycheck bro, everyone's looking forward to it.*" Later, reminding his superior:

> *"Pay the gang here bc1qkmyv5860pe24h9ytadkzgqltkjuuk9z9s027df*
> *sum total 85k*
> *99947 core team 62 people, I get 54 paychecks*
> *33847 - reverse team, 23 people*
> *8500 - new team of coders, 6 people, only 4 are getting salaries so far*
> *12500 Reverses, 6 people*
> *10000 OSINT department 4 people*
> *3000 for expenses (servers/protections/ test tasks for new people)*
> *164.8k total per month."*

In addition to operating under a hierarchical structure, there is a **division of labor** within the Conti network. The chat logs are replete with mentions of teams with different designations: teams of coders, core team, reverse team, and OSINT department. From the chat data, we know that numerous individuals are mentioned occupying certain roles, such as a message from *Stern* to *Mango* in which *Stern* mentions "HR managers *Salaman*, *Kagas*, and *Viper*" or many others naming individuals as "team leads."

Conclusion

Based on our analysis of the Conti chat network, we have explored the patterns of interactions between nodes to reveal a hierarchy. Based on the data, there are several members that are the most connected. While there is still much to be discovered about Conti

leadership, knowing the overall inner workings of communications, projects, and deliverables within ransomware structures offers new opportunities to disrupt their operations and avoid them altogether.

This leak provides insight into the structure of ransomware groups and the non-technical elements driving the ransomware business. Analysis indicates that individuals within the Conti threat actor group are still responsible for technical and financial responsibilities. Rather than a one-off, lone wolf operation, our analysis reveals a possible core group of 44 individuals who run the Conti operation.

Conti is armed with a human team, hierarchy, and structure of responsibilities as outlined in their chats and as investigated first-hand by Tetra Defense, an Arctic Wolf company. Being a human-driven enterprise, ransomware provides periods of time between victim discovery, initial access, reconnaissance, and attack deployment when an attack can be disrupted. While the future of the Conti group remains uncertain, this leak provides a case study on the inner workings of a Ransomware as a Service (RaaS) structure — a common structure used by other threat actors we investigate daily.

With the Conti group still operational, the threat remains, as evidenced by the sprawling network of members and affiliates. This deep analysis provides us a unique understanding in adversary operations, and informs how we build and enhance our detections to anticipate future TTPs and tradecraft. Arctic Wolf works side by side with customers, 24x7, to hunt for activity and deploy new detections—always advancing security operations with threat intelligence and analysis to fuel into the Arctic Wolf® Platform.

This analysis was performed by Tetra Defense, an Arctic Wolf company, in collaboration with Arctic Wolf Threat Intelligence.

---

[1]Edges in directed networks are often called arcs, however, for simplicity sake we will refer to them as edges in this analysis.

[2]Vincent D Blondel, Jean-Loup Guillaume, Renaud Lambiotte, Etienne Lefebvre, Fast unfolding of communities in large networks, in Journal of Statistical Mechanics: Theory and Experiment 2008 (10), P1000

R. Lambiotte, J.-C. Delvenne, M. Barahona Laplacian Dynamics and Multiscale Modular Structure in Networks 2009

[3]This is the network's K-Core.

[4]We are using the unweighted degree to establish sending and receiving relationships and thus filter nodes for which a larger number of messages are exchanged in aggregate. While the latter can be a useful measure, technical collaboration may require a higher volume of

communication. For transparency, Bentley had the highest weighted in-degree, followed next by Stern. Yet, Bentley had the fewer total individuals from which these messages originated.

[5]Mango and Buza were not among the top 5 on PageRank.

[6]This is based on Jon M. Kleinberg work, “Hubs, Authorities, and Communities”

(http://www.cs.cornell.edu/home/kleinber/auth.pdf) and “Authoritative Sources in a Hyperlinked Environment” (http://cs.brown.edu/memex/ACM_HypertextTestbed/papers/10.html)

[7]For more detail, see the original paper here: http://ilpubs.stanford.edu:8090/422/. In this paper, weighted PageRank was used, taking into account edge weights.