控制論的戰爭。

分析Conficker蠕蟲，Stuxnet病毒，Duqu約火焰，火焰小，高斯，馬赫迪Shamoon

信息安全論壇

www.gocs.de - 歐盟信息com.de

節略版

我們第一次簡單的問題，因為實際上已經開始了嗎？

這個問題可以很容易地回答“是”和“否”。

要回答這個問題，我們甚至不屑於評價新聞發布的主題。

對於那些誰想要指責我們，我們將使用“信息，秘密zuhaltende”。讓我們再次強調，我們只分析可公開獲得的材料。

分析期間，我們只用期“Stuxnet的Shamoon，”這是一個相對短的時間內。

同時，廣大人民群眾的惡意軟件方面的限制。因為它僅僅是典型的“控制論箭”，以滿足“武俠”的屬性。

但是，在相同的時間，典型的結構，這是典型的武器系統。但單兵武器系統的時間依賴關係。

雖然很少有“控制論箭”充分說明，他們讓一個非常有趣的見解。在哪裡可以看，我們寫的，否則就失去了連接。由於搭載了枚不能建立一種戰略防禦或防禦。這當然前提是他們想要的。

組在此期間應控制論武器的間諜裝置的破壞的裝置是已知的它們，或者假定為已知設置。

我們已經把他們分成兩組。

其中一組包括銷毀和破壞的武器。

另一組則包含間諜系統，子系統，和一些，如操縱系統。

根據這一子類別操縱系統，方法應被理解為被改變的信息存儲或刪除。然而，沒有生產控制系統。

第一組

最有名的代表該組的“Stuxnet蠕蟲”和“Shamoon”。它們的作用是編程過程中系統的破壞。（Stuxnet病毒），而且在計算機基礎設施的破壞，如磁存儲（硬盤驅動器）等。

其特徵在於由一個非常具體的銷毀模塊的第一個著名的控制論箭頭。這需要特殊的生產控制系統（鈾濃縮系統中的PLC西門子）。

使用時，對來自同一製造商的其他生產控制系統嚴重損壞。

第一次使用這種控制論箭頭的特點是一個特殊的功能。這是第一個選擇性地使用 - 那就是 - 通過直接實施控制論系統（計算機）的攻擊。據各種媒體報導，這兩起襲擊進行了授權的員工在各自的計算機中心。

這關係到伊朗的攻擊，以及攻擊在沙特阿拉伯，那裡的石油業遭受沉重打擊。

何種程度上內部的保安措施，減少他們的損失，不知道。

從通信系統（互聯網或其他溝通渠道），因此任何防腐劑是不能奏效的。基於互聯網的安全性措施在這樣的攻擊是無效的（所謂的網絡防禦司令部）。

這是使用“Stuxnet的”和“Shamoon”都同樣如此。

這些感染，有多少被授權的員工是未知的。對於這種類型的攻擊只發生這個直接到計算機系統中的重要性。

此類型是直接在計算機系統中或相應的操作系統和更嚴格的保護措施，如內部編碼或加密，需要一個保護系統的類型。在已知的保護系統分開。這意味著什麼，這些系統必須根據信息的價值。

的情況下，在第一次使用後發生集體感染，即使是通過互聯網的“Stuxnet蠕蟲”。它應該被感染約60,000個單位。應該是怎樣分佈的目的，這是不清楚，“Stuxnet的”高度專業化的控制論箭，仍然是。

當時的孔中的軟件系統只用了很長一段時間後，填補了數個月。

進行了這個“Flickenschusterei”，控制論的戰爭（網絡戰）已經成功地執行這些孔。

壓頭，使一個非常聰明的入侵。的繼承人或在同一個平台的產品使用的各種穿甲彈。

孔比有多少！

強調，即使在目前的結果，從一個事實，即只有相關的有害模塊需要被替換為其他的目標特性。

相同的行為，也適用於“穿透”滲透到各自的控制論單元（計算機系統）。

的模塊化是現代控制論箭的一個特點。

第二第二組是更為廣泛。已知的代表Duqu，火焰，高斯，迷你火焰和Mahdi。

這個組可以描述為“控制論間諜”。這種控制論的間諜標有間諜的經典特徵。

這是特殊的，控制論更詳細的情報。

控制論的間諜非常不同。特此設立代表Duqu和Mahdi只在少數。這意味著無非的這些控制論箭頭的相對較少的，什麼都可以的情況下，很少有發現。的特殊任務，這也意味著小有名氣。然而，他們被認為是“非常危險”。太陽特別是也對BSI /德國。從其他來源，長期使用不排除與新間諜模塊。

它可與一個Duqu偵察衛星。他是在那裡，但另外一個不知道！

它必須承擔與重新使用這些數據源。根據已知的各種平台的發展經驗，“Duqu和Stuxnet”更先進的系統。

即使這條線的發展是顯而易見的，在已知的間諜系統。

還發現平台 - 原理應用。這意味著什麼，以及測試和驗證系統的開發，通過使用新的模塊類型的任務。的經驗的同時，可以與舊的解決方案修改和優化，以滿足不斷增長的需求。分析涉及的模塊以及通信模塊。後者是特別重要的，因為他們贏得了必須將信息傳遞到隱藏的服務器。這適用於的信息量以及為保密。出於這個原因，“恢復的信息”中的加密或加密的形式發送。同樣的原理也被用於第二次世界戰爭。因此，從“謎”，編碼為進一步傳播獲得的信息。的英方使用什麼程序來似乎仍然是一個謎。這整個過程得到了“超”的名稱。

這防止，德方獲得的知識，而“崩潰”之謎加密系統的解密信息的保護。這也給了一個比喻，在八十年代的背景下，信息的ex.DDR ZCO解密。

這種老方法檢測到，即使在控制論的間諜。同樣，信息是受保護的，因此沒有遠見的間諜的信息。另外，在關於此信息，發送從發送到服務器，而不是“有趣的信息的引導。”

控制論的對象，這是闡明本控制論箭應該沒有顯著的證據表明，信息澄清的重要性。

同樣，有一個非常有趣的方法：

（1）

一些買家買了“磁介質”，有趣的，有價值的信息（如稅收數據為德國逃稅者）和€支付數百萬。這個信息的價值是多重的。

市場上的信息一般人都知道，歐洲的金融機構尋找“貨幣乘數的信息”。

此信息將不能在市場上出售，他們將只提供給“非法”。這些行為所進行的“獲授權人士”。

（2）

獲取信息的另一種形式，它需要使用控制論劑優選別人。

在這種情況下，假定的箭頭控制論在陌生的控制論系統的信息收集器的功能。這裡收集的信息將被發送通過通信服務器。在某些情況下，數據將被轉發由Massive 5千兆字節的大小。然而，它們可以更大或更小。

通過“控制論箭頭”是數據收集相比更加靈活，因為一個人源。這些箭頭的使用允許的客戶端對應的理想的適合給予答案。

如下，當然，它的優點是，你可以快速的變化，因為主體，已發現了另一種來源不明。

在肯定聽說過智能控制論的特點，在目標的快速變化。

不同的方法都依賴於政府的各自形式。

這些小Spionagehelferlein，就像任何其他程序或控制論的箭頭大小。這些修長，而另一些大的船。他們來自同一個平台。

其中最有名的“大舟”是“火焰”。

控制論的間諜使用的是非常不同的。

因此，一些Duqu或小火焰只可用於小批量。據預計為每個系統最多到60感染。

因此，這些特殊的控制論間諜的總數是約120感染。

這似乎是一個高度特異和敏感的控制論的間諜。

不能提供的信息進行分析評估。

然而，其他人可以適量使用。雖然發現感染率在10,000或更多。

火焰感染約5000至6000

高斯約2500名感染

邁赫迪大於700感染

Conficker蠕蟲約60,000或可能更大。

這些控制論間諜的應用率高達10倍至100倍以上的特殊系統。在某些情況下，這個值可以超過顯著（Conficker）蠕蟲。

不同的感染面積68 200和從最小的和最多可達100,000或更多感染。

真正的數字要高得多。從其他有害系統的分析，可以假設因素之間的3 ... 8。

不明的情況下的高數量的原因是已知的，將不再進一步討論。

在地理分佈的“惡意程序”在這裡故意未指定要處理的。由於數量的應用程序的控制論箭頭供給其他不同的結果。同時，在地緣政治的某些控制論箭的使用是不合邏輯的。

一個非常有趣的一點是在哪些領域，政治，經濟，軍事，研究和開發，基礎設施等專用的分析Fragegestellung的

他們的研究結果是非常有趣的。

這些結果沒有公佈的“誤解”大事化小和控制論的戰爭絕不是危言聳聽，可能會導致世界末日。

在此之前分析2012年12月10號

注：

這種材料的“信息安全論壇”的一部分。

有出版，並不斷更新。

這種材料只可公開獲得的出版物。

在互聯網上公佈，在以下地址：

www.gocs.de 或去 www.gocs.eu 的或 www.gocs.info 或 www.gocs.com.de 的

2012年12月23號柏林,

作者老GOCS

作者許可，重複使用。這種分析將不斷更新。錯誤。